



# **SecureOffice® Trusted Workstation™ Administrator Training**

## **Module Two: TCS Administration Tools**

- TCS System Administration Tools
  - System Accreditation Levels
  - Network Interface Definition
  - NIS+ Specification
  - NIS+ Recovery
  - Gateway Router Configuration
  - Domain Name Service Specification
  - Remote Hosts Definition
  - IP Filtering Administration

- TCS System Administration Tools
  - Software Version Description
  - Default Editor Specification
  - System Backup
  - Audit Backup
  - VFind Virus Definition List Update
  - VFind License Verification
  - Audit Reduction Tool
  - File Type Customization
  - Alternate File Type Configuration
  - File Type Viewer

# SecureOffice TWS

## Administrator

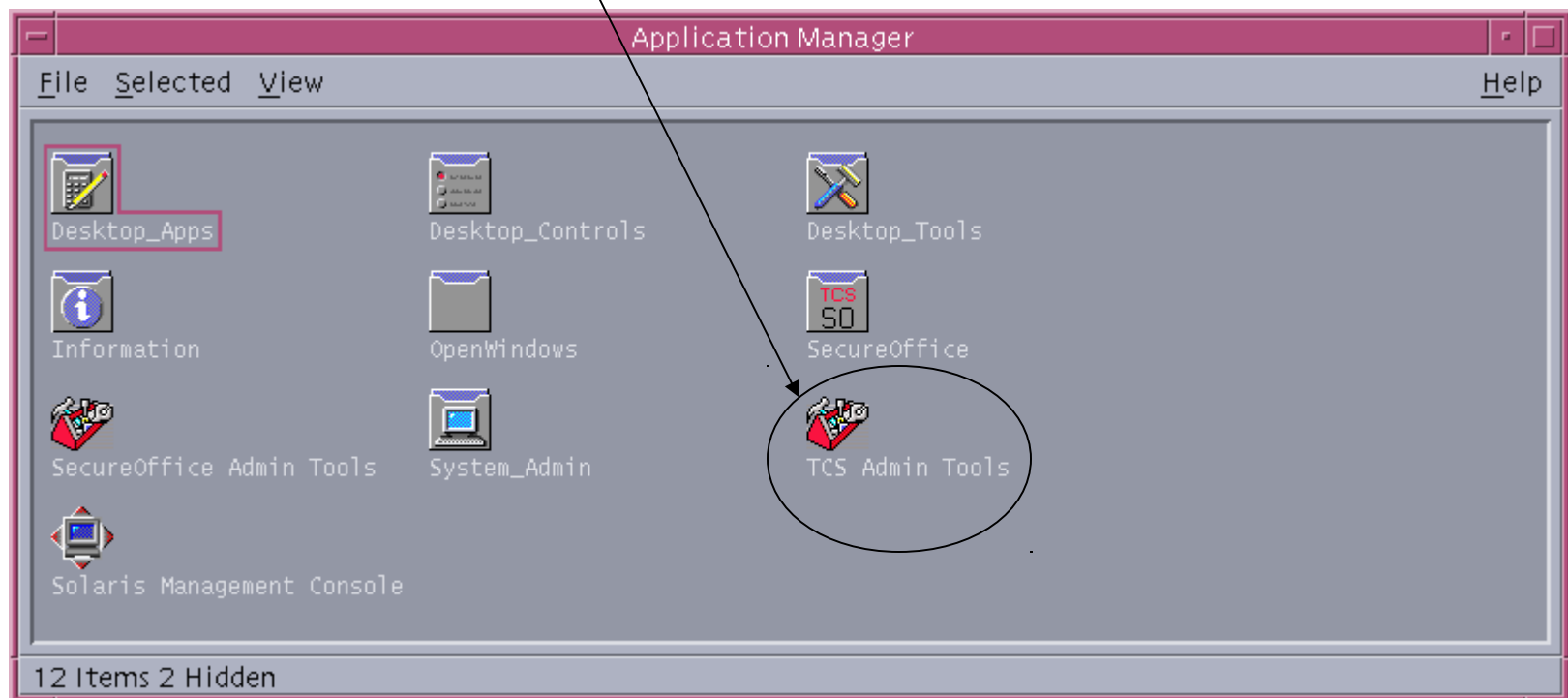
### TCS System Administration Tools

- Accessing TCS Admin Tools
  - Trusted Solaris **root** role is configured to execute all TCS Administration Tools
  - TCS provided System Administration Tools require a valid system license to operate.
    - If none of the tools will operate, you should confirm that the license key you have entered is correct. This can be verified in a console window.
    - Contact TCS for a valid license key.
  - Assume Root Role
    - Select or add root role workspace
    - Launch Application Manager with left single-click on Application Manager icon



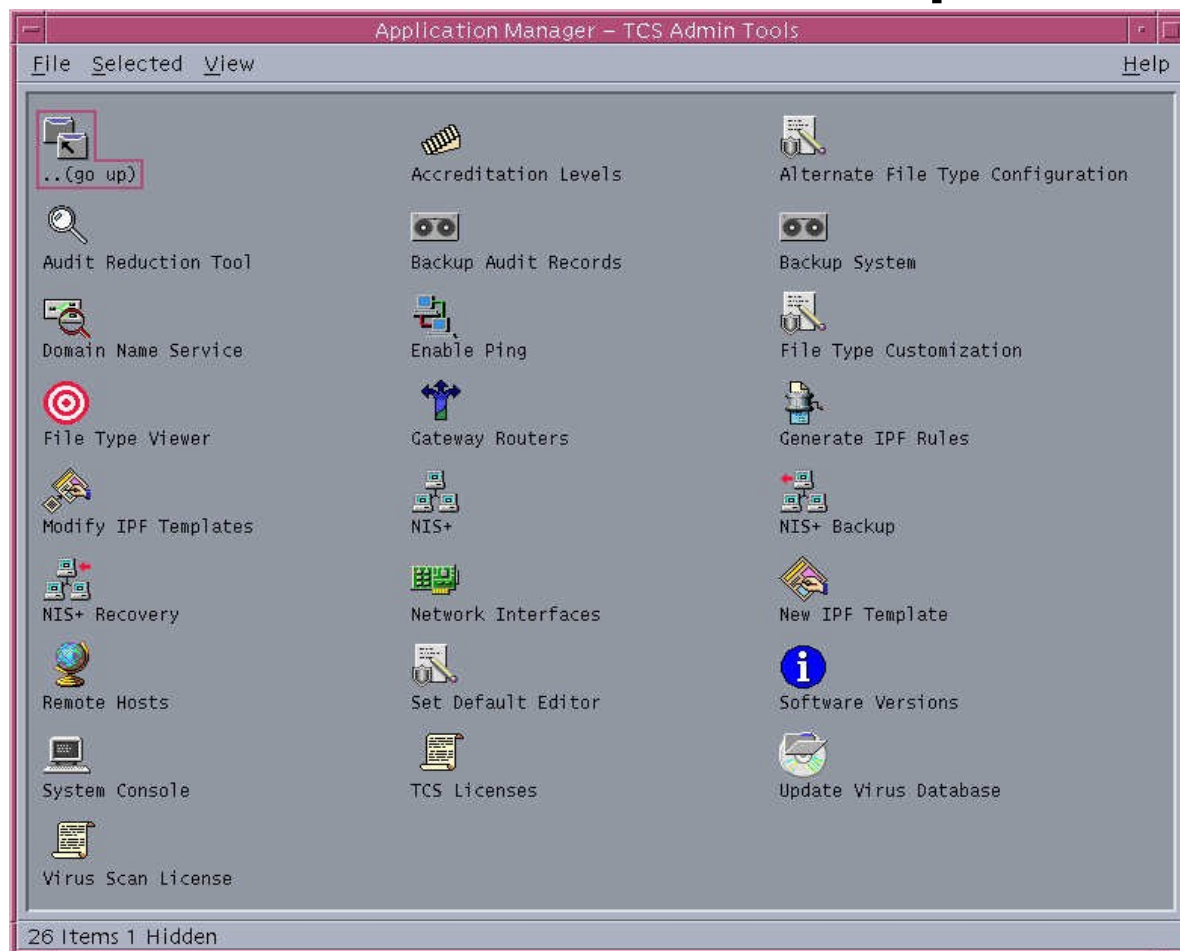
# SecureOffice TWS Administrator TCS System Administration Tools

- Accessing TCS Admin Tools (con't)
  - From the Application Manager Desktop, left double-click the TCS Admin Tools icon.



# SecureOffice TWS Administrator TCS System Administration Tools

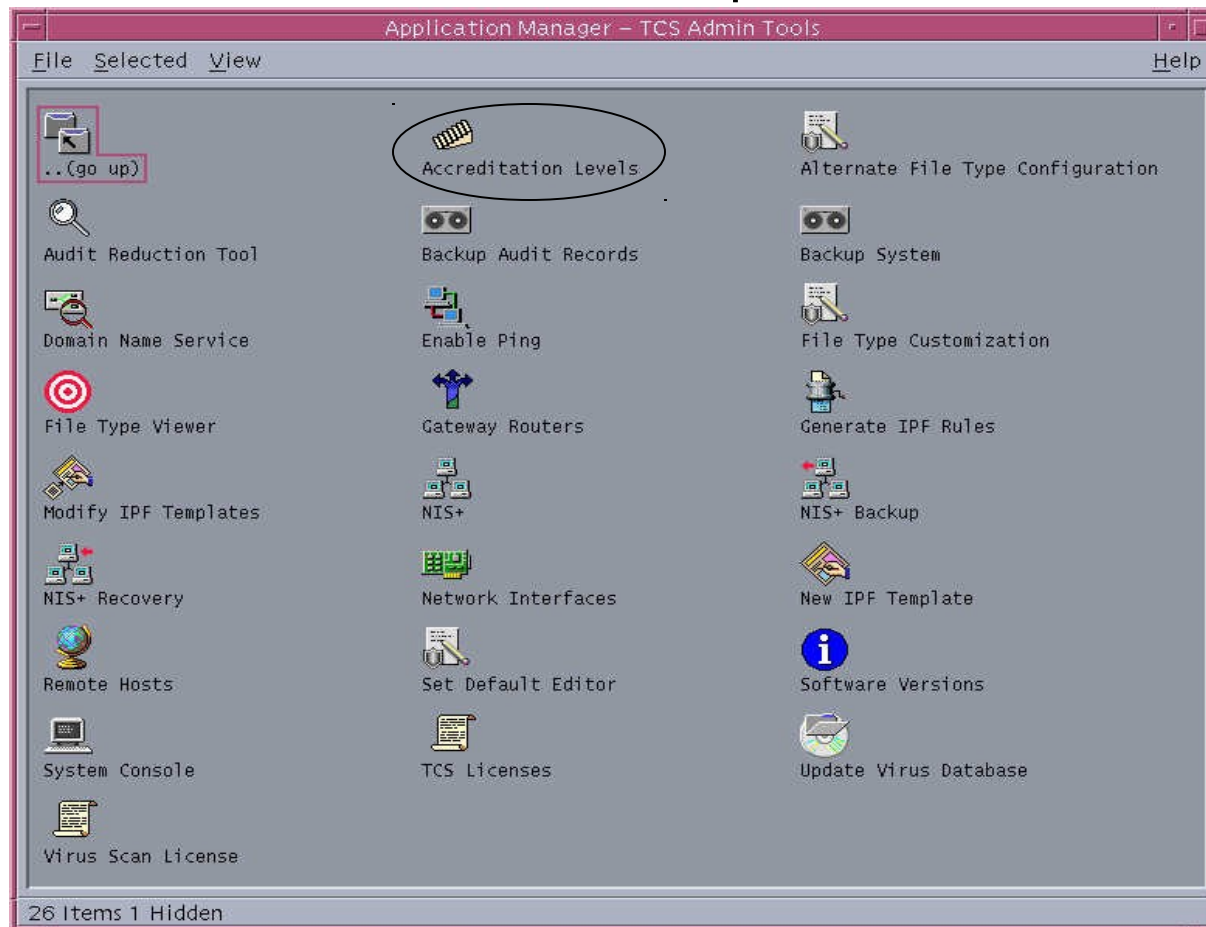
## TCS Admin Tools Desktop





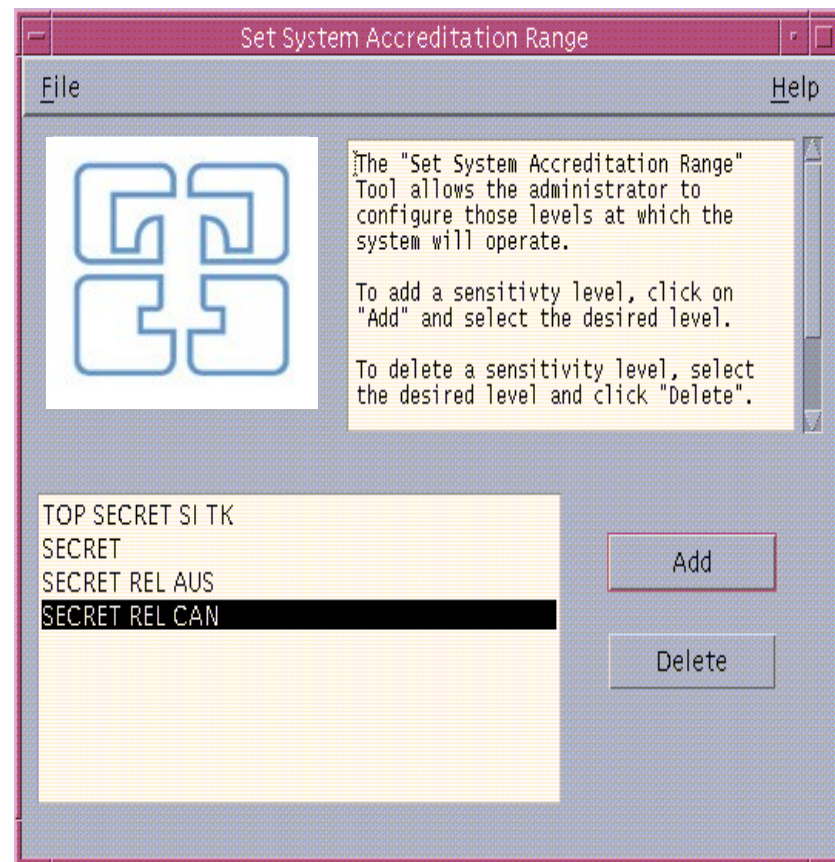
# SecureOffice TWS Administrator TCS System Administration Tools

## Accreditation Levels Specification Tool

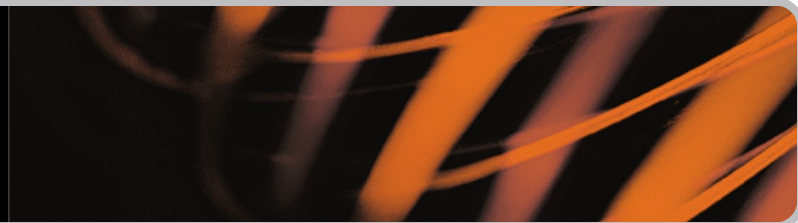


## System Accreditation Tool

- Execute the **Set System Accreditation Range** tool, with a left double-click on the **Accreditation Levels** icon.
- The **Set System Accreditation Range** tool sets up the sensitivity labels from the system encodings file which are to be used on the system.
- These labels are used by the other TCS System Administration tools as the sensitivity labels presented in the SL list boxes
- Should at least include all sensitivity labels for all network interfaces to be configured on the system.



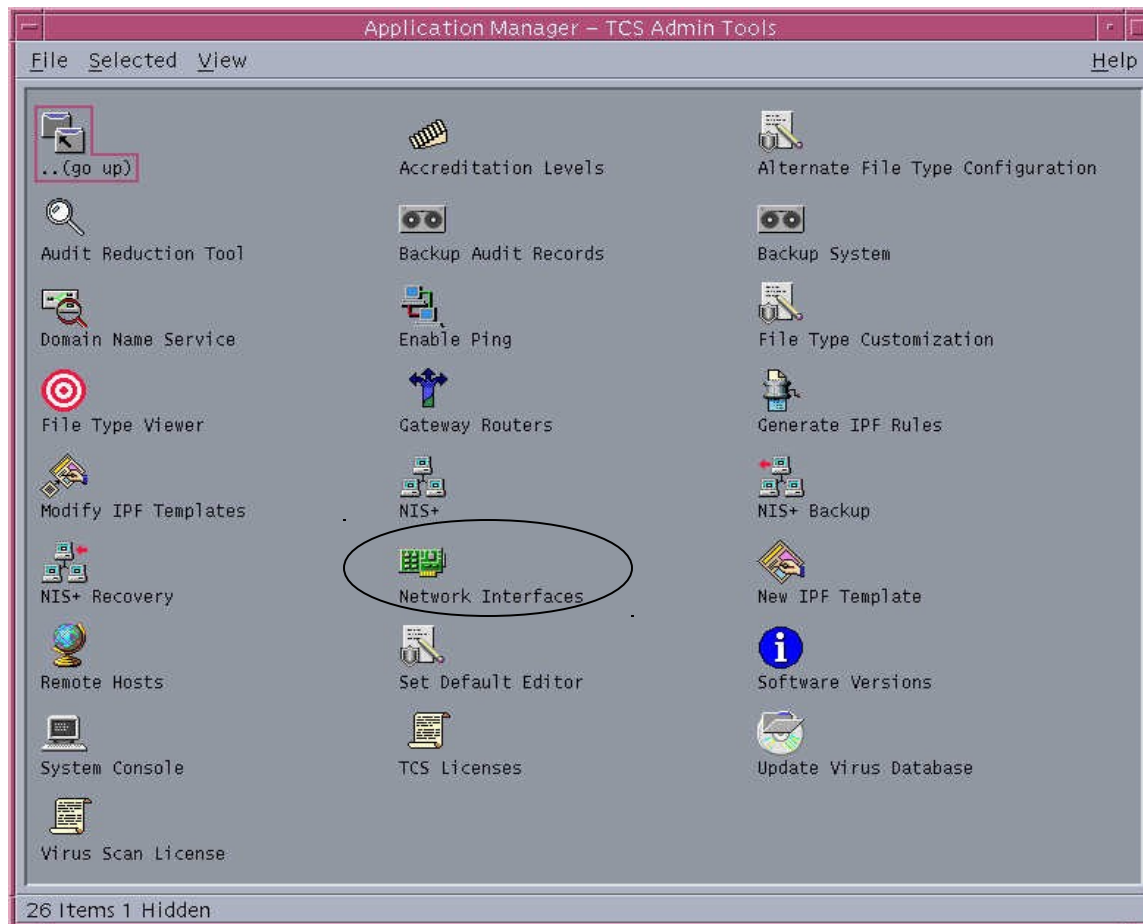




- System Accreditation Tool (con't)
  - **Add** Button
    - Pops up Sensitivity label selection tool
    - Specify Appropriate Label
    - Adds specified label to tool list
  - **Delete** Button - deletes highlighted entry in tool list.
  - **File** menu
    - **Save** - Save and configures current settings in tool
    - **Save and Exit** - Saves and configures current settings to system configuration and exits tool
    - **Exit** - Exits tool without saving changes.

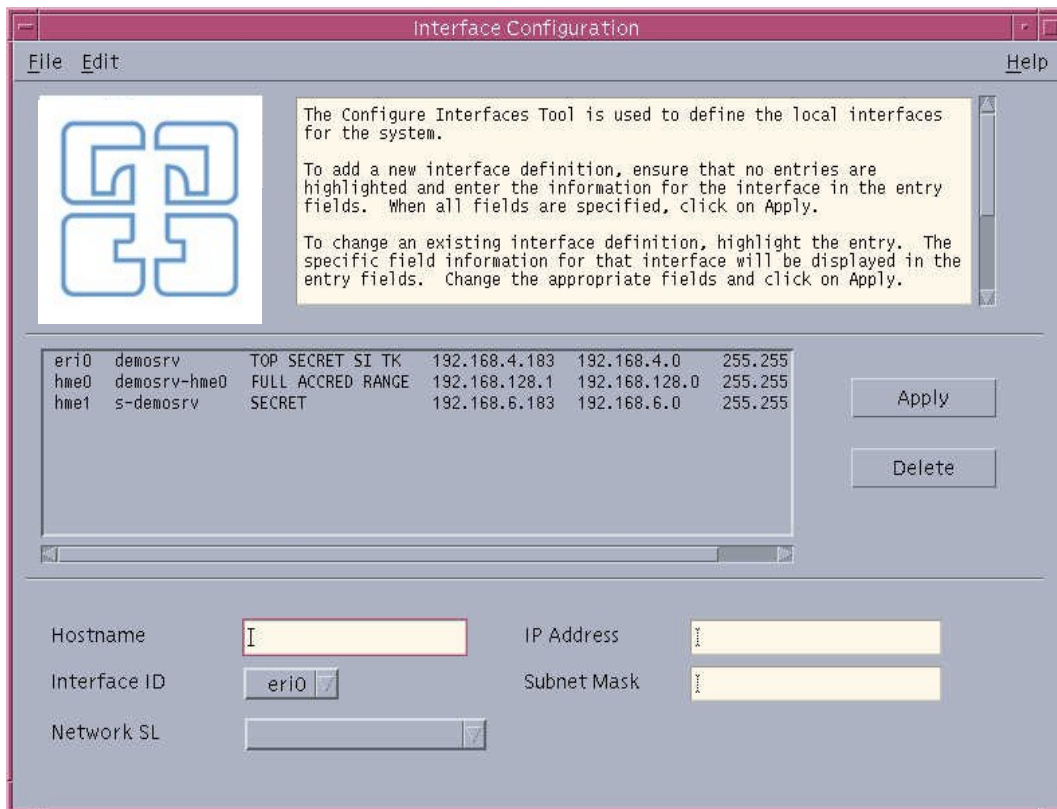
# SecureOffice TWS Administrator TCS System Administration Tools

## Network Interfaces Definition Tool



## Network Interface Configuration Tool

- There are typically multiple interfaces on SecureOffice
- All fields are mandatory
- Each Interface has traditional IP related attributes
  - Hostname
  - IP Address
  - Interface ID
  - Network Subnet Mask
- Each Interface has security related attributes
  - Network SL



Interface ID	Name	Security	IP Address	Subnet Mask	Netmask
eri0	demosrv	TOP SECRET SI TK	192.168.4.183	192.168.4.0	255.255
hme0	demosrv-hme0	FULL ACCRED RANGE	192.168.128.1	192.168.128.0	255.255
hme1	s-demosrv	SECRET	192.168.6.183	192.168.6.0	255.255

Hostname:

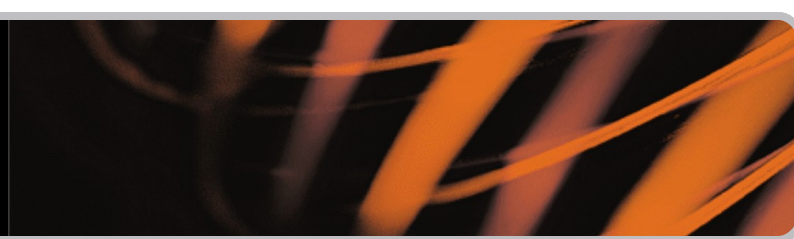
IP Address:

Interface ID:

Subnet Mask:

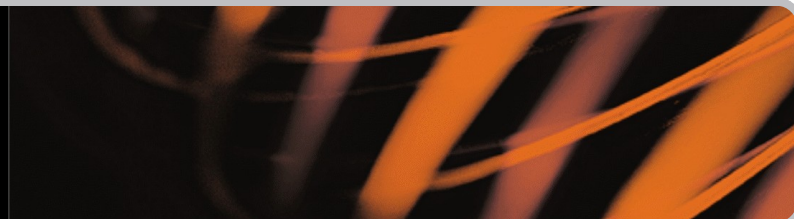
Network SL:

- Network Interface Configuration Tool (con't)
  - Hostname
    - This will be the name that you and others should know this system by. Each interface has a unique hostname associated with it.
      - » A common convention is to call the HIGH interface the primary interface and associated with the primary hostname. (Ex. **station1**)
      - » The LOW interface hostnames commonly have names like **station1\_secret**, **station1\_srel4**...



- Network Interface Configuration Tool (con't)
  - IP Address
    - Address assigned to the interface in IP format X.X.X.X, where X is between 0 and 255.
  - Interface ID
    - The hardware identifier assigned to the interface. Examples are hme0, le0, qfe0, etc.





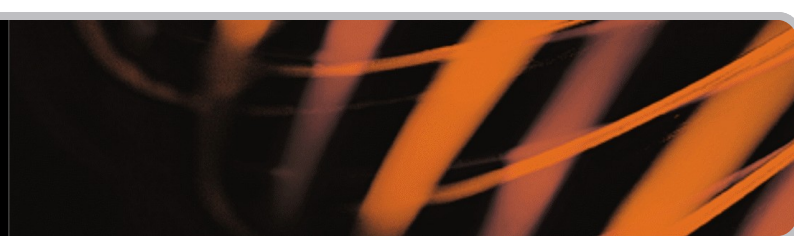
- Network Interface Configuration Tool (con't)
  - Network SL
    - This is the Level at which data obtained over this interface should be labeled. The HIGH level network must be configured as “Full Accred Range”. All other [LOW] interfaces should be configured as LOW; where LOW is the Sensitivity Label of all data on that network.
  - Network Subnet Mask
    - The subnet mask is the means by which a network can be subnetted over a common network IP address. Consult your Network Admin. This field can be used to subnet your class A,B,or C network address. Subnetting class ‘C’ networks is very common. Typical class ‘C’ subnet examples follow.

- Network Interface Configuration Tool (con't)

- Sample Class 'C' Subnet masks

Bit	Network Mask	Subnets
256	255.255.255.0	1
128	255.255.255.128	2
64	255.255.255.192	4
32	255.255.255.224	8
16	255.255.255.240	16
8	255.255.255.248	32
4	255.255.255.252	64
1	255.255.255.255	0*

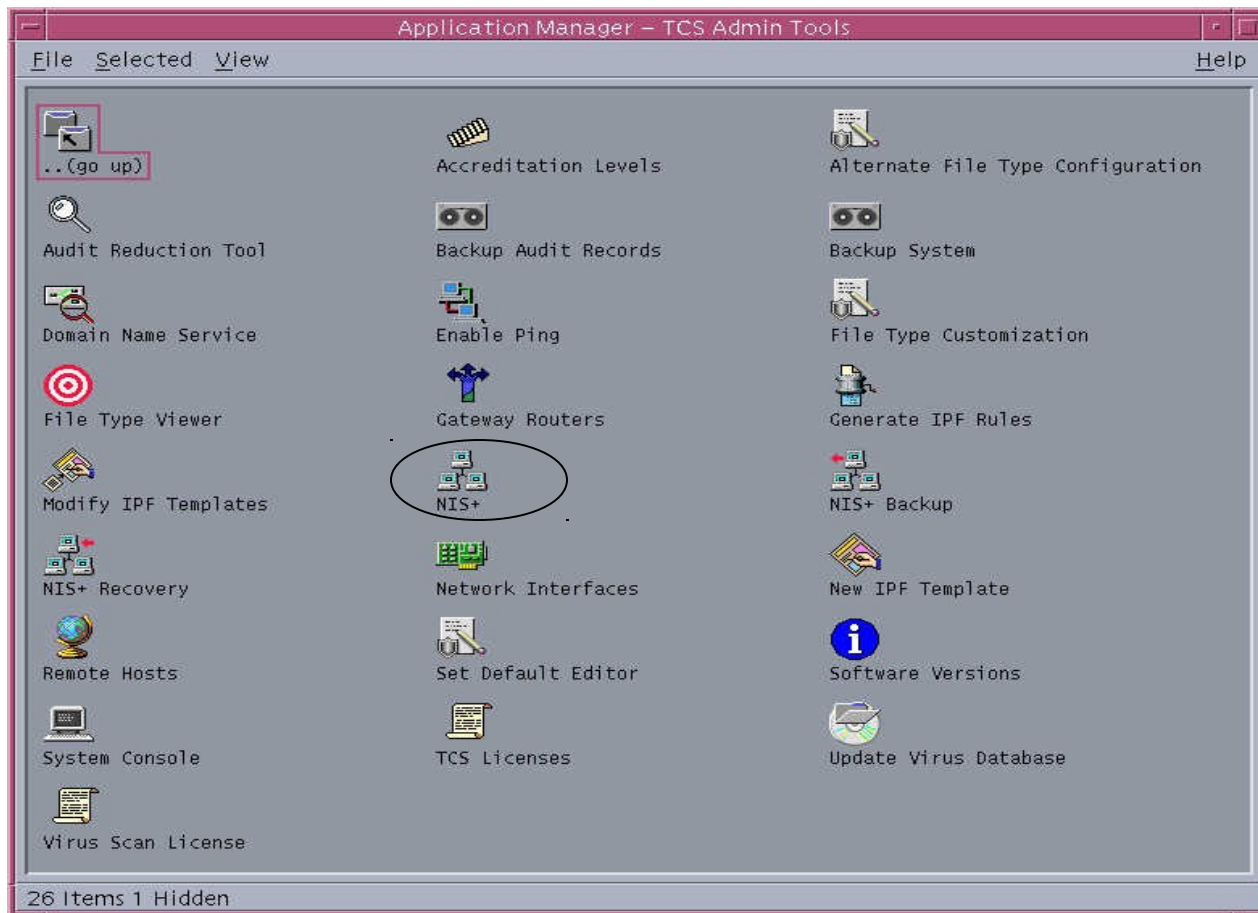
- Tool handles Class 'C' subnet mask with all one's in the last octet as if it was set to zero, meaning no subnets.
- Not limited to a Class 'C' subnet. (ie- 255.255.252.0)



- Network Interface Configuration Tool (con't)
  - Interface Tool
    - **Add** Button - adds entry to tool list.
    - **Delete** Button - deletes highlighted entry in tool list.
    - **File** Menu
      - Save - Save and configures current settings in tool
      - Save and Exit - Saves and configures current settings to system configuration and exits tool
      - Exit - Exits tool without saving changes.
    - **Edit** Menu
      - Copy - Makes a copy of the currently selected host or wildcard configuration for modification
        - » Useful when adding a host or wildcard entry that is similar to an already existing host or wildcard entry.

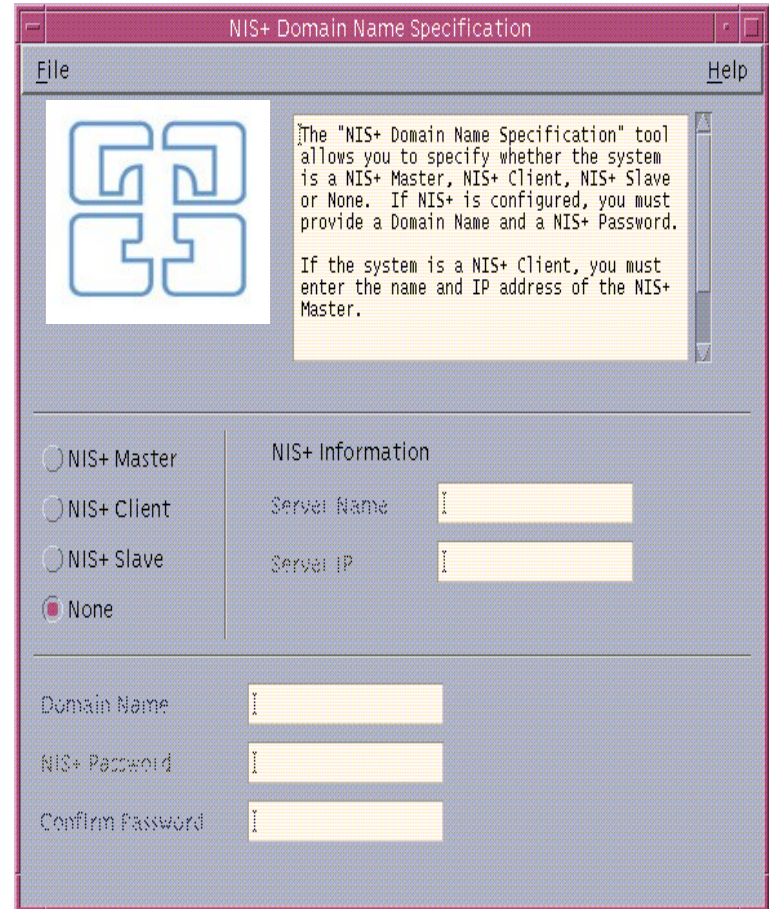
# SecureOffice TWS Administrator TCS System Administration Tools

## NIS+ Definition Tool



## NIS+ Specification Tool

- Only one NIS+ Master Allowed
- NIS+ Slave Server Supported In Future Release
- Multiple Clients Allowed
- NIS+ Domain Name Specification
- NIS+ Secure RPC Password specification
- NONE is for a stand-alone non NIS+ architecture.



The screenshot shows a window titled "NIS+ Domain Name Specification". It features a menu bar with "File" and "Help". On the left is a logo consisting of four interlocking squares. A text box on the right explains the tool's purpose: "The 'NIS+ Domain Name Specification' tool allows you to specify whether the system is a NIS+ Master, NIS+ Client, NIS+ Slave or None. If NIS+ is configured, you must provide a Domain Name and a NIS+ Password. If the system is a NIS+ Client, you must enter the name and IP address of the NIS+ Master." Below this, there are radio buttons for "NIS+ Master", "NIS+ Client", "NIS+ Slave", and "None" (which is selected). To the right of these are input fields for "Server Name" and "Server IP". At the bottom, there are input fields for "Domain Name", "NIS+ Password", and "Confirm Password".



- NIS+ Specification Tool (con't)
  - Prior to using NIS+ Domain Name Specification tool
    - » Configure the NIS+ Master to recognize all NIS+ Clients
    - » NIS+ Master and each NIS+ Client must be configured to have a Network SL of **FULL ACCRED RANGE** and a Protocol of sun **tsol** to enable NIS+ communications.
    - » IP filtering must be configured to allow all IPC communications between these systems.
    - » Uncomment or add the following entries to allow all traffic between the NIS+ Master and NIS+ Clients on the high side in the high side interface filter configuration file.  
Change REMOTEIP to the IP Address of the NIS+ Master.

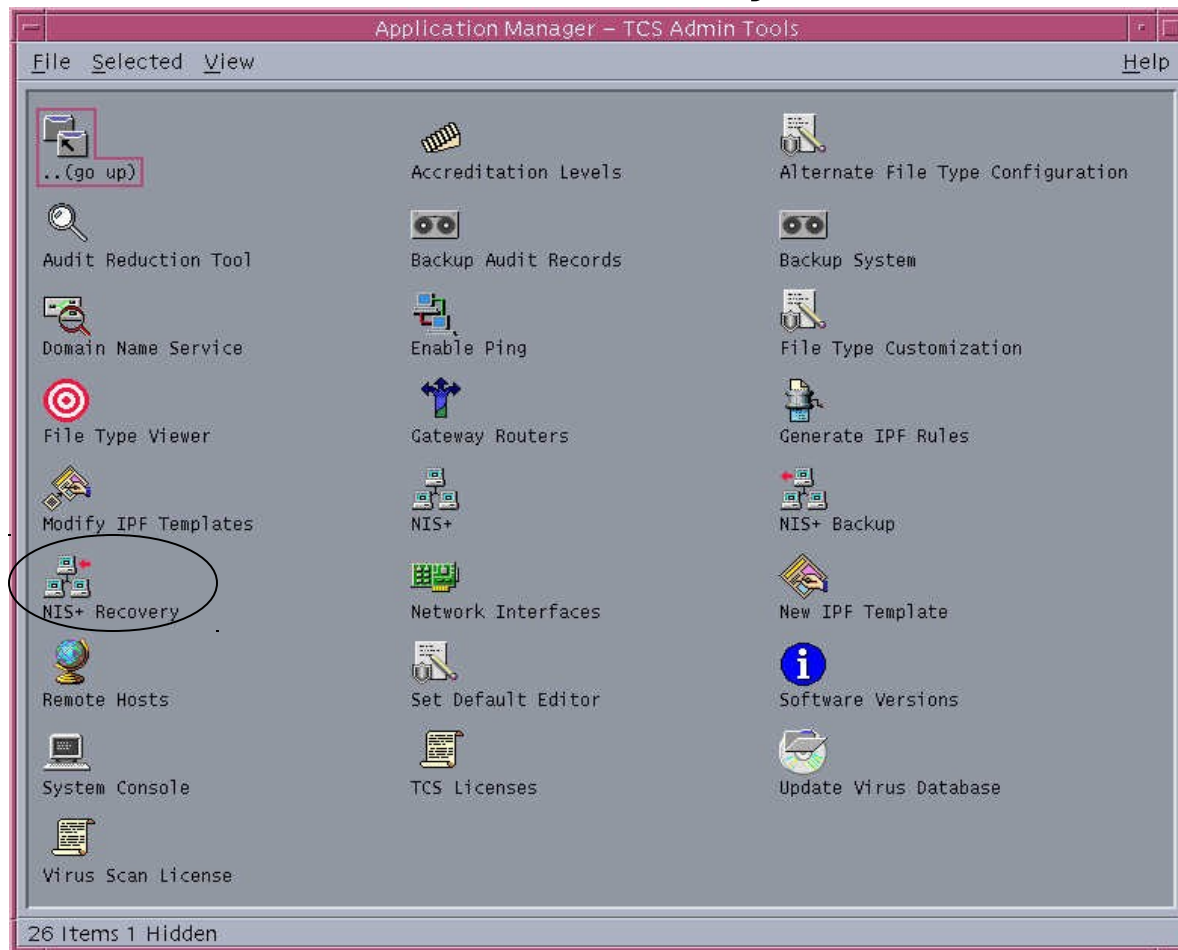
```
/etc/security/tcs/high-ipf.conf
```

```
# <---> allow NIS+ incoming/outgoing between systems
pass out quick on IFC from ADDR to REMOTEIP
pass in quick on IFC from REMOTEIP to ADDR
```

- NIS+ Specification Tool (con't)
  - **Specify NIS+ Host type**
    - NIS+ Master - This system will be configured as an NIS+ Master
      - » Requires NIS+ **Domain Name**
      - » Requires NIS+ Password
      - » Requires NIS+ **Confirm Password**
    - NIS+ Client - This system will be configured as an NIS+ Client
      - » Requires NIS+ **Information Fields**
      - » Requires NIS+ Master **Server Name**
      - » Requires NIS+ Master **Server IP** address
    - NIS+ Slave - Not currently supported.
    - None - No NIS+ is configured

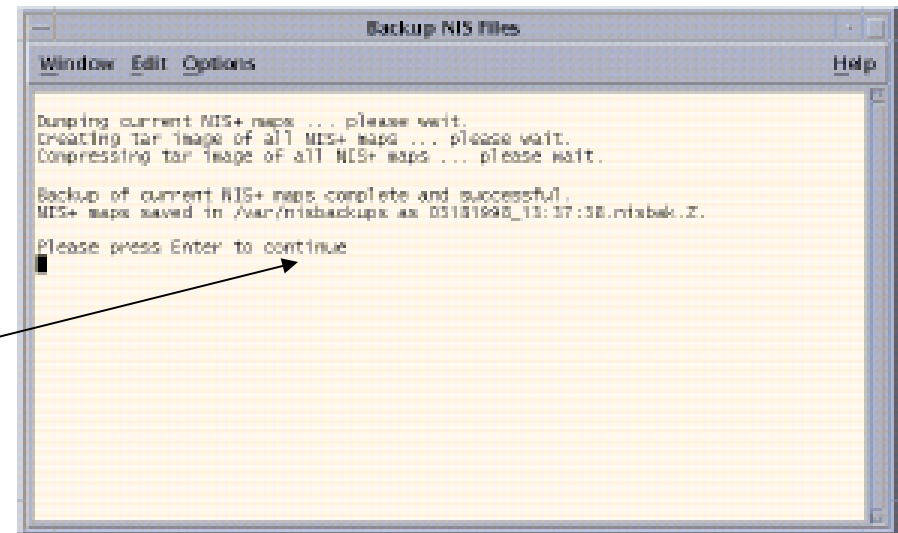
# SecureOffice TWS Administrator TCS System Administration Tools

## NIS+ Recovery Tool



# SecureOffice TWS Administrator TCS System Administration Tools

- NIS+ Backup/Recover Files Tool
  - Backup NIS+ Files tool
    - Only Run on NIS+ Master
    - Log files are maintained in:  
`/etc/security/tcs/logs`
    - Name of the file containing the backup maps is displayed in the tool.



The screenshot shows a terminal window titled "Backup NIS Files". The window has a menu bar with "Window", "Edit", "Options", and "Help". The text in the terminal reads: "Dumping current NIS+ maps ... please wait.", "Creating tar image of all NIS+ maps ... please wait.", "Compressing tar image of all NIS+ maps ... please wait.", "Backup of current NIS+ maps complete and successful.", "NIS+ maps saved in /var/nisbackups as 03181848\_13:37:38.nisbak.Z.", and "Please press Enter to continue". A cursor is positioned at the end of the last line. An arrow points from the text "/etc/security/tcs/logs" in the list to the terminal window.

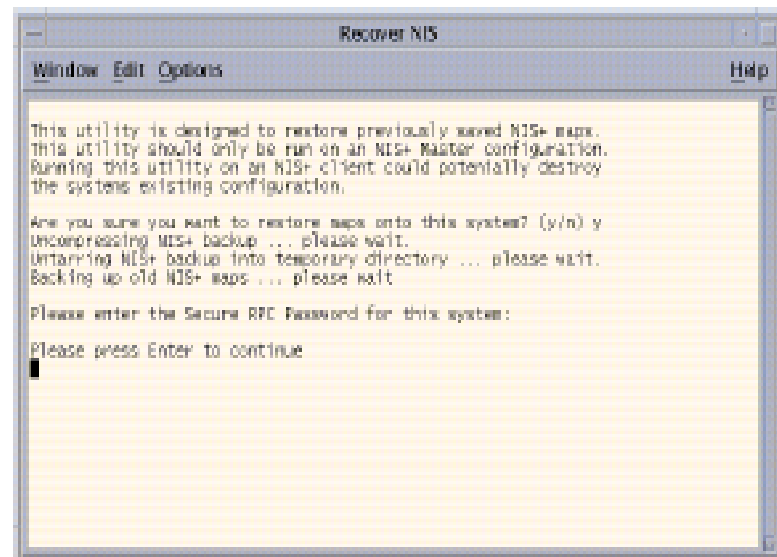
```
Backup NIS Files
Window Edit Options Help
Dumping current NIS+ maps ... please wait.
Creating tar image of all NIS+ maps ... please wait.
Compressing tar image of all NIS+ maps ... please wait.
Backup of current NIS+ maps complete and successful.
NIS+ maps saved in /var/nisbackups as 03181848_13:37:38.nisbak.Z.
Please press Enter to continue
```

# SecureOffice TWS

## Administrator

### TCS System Administration Tools

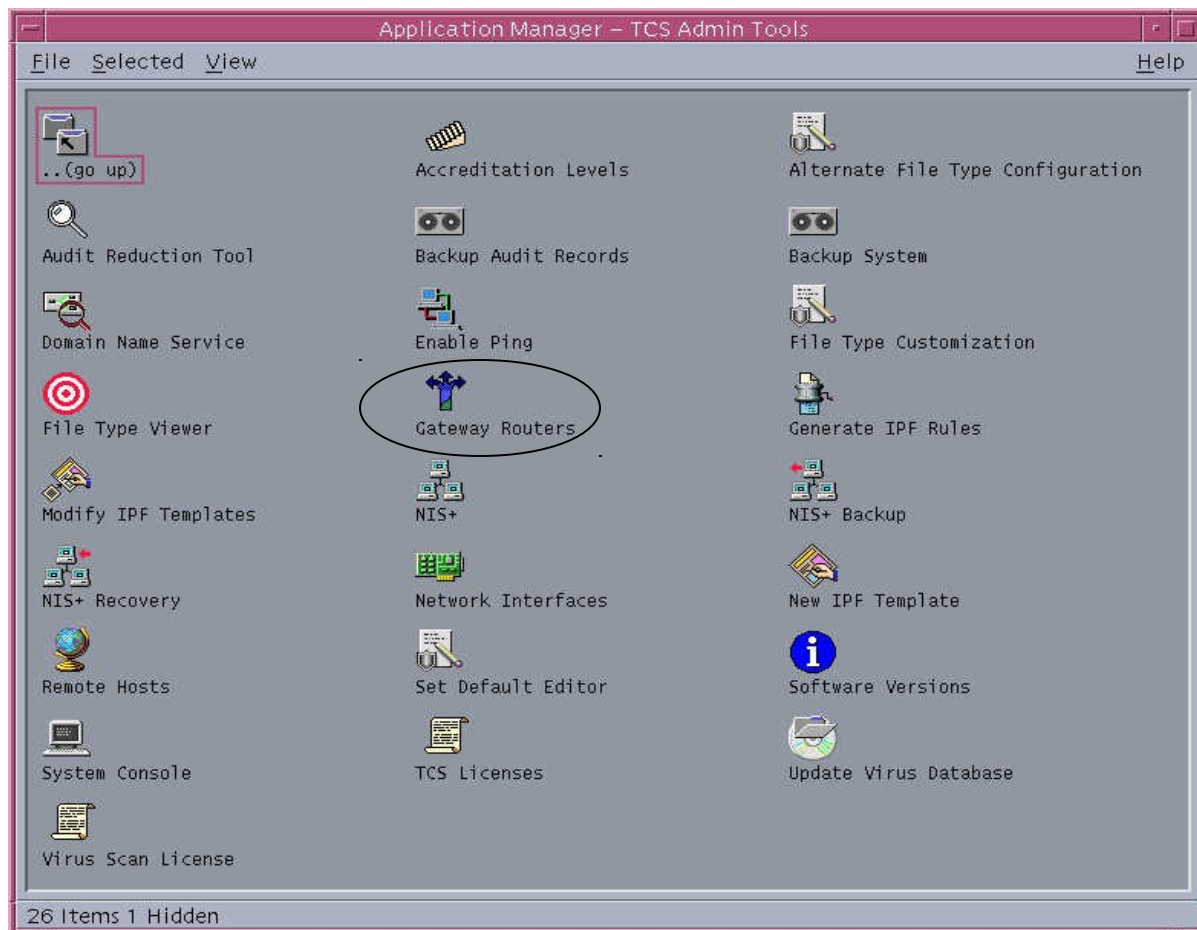
- NIS+ Backup/Recover Files Tools (con't)
  - Recover NIS+ tool
    - Restore NIS+ files that have been previously backed up.
    - Log files are maintained in:  
`/etc/security/tcs/logs`
    - Enter the NIS+ backup file name
    - Enter NIS+ Password





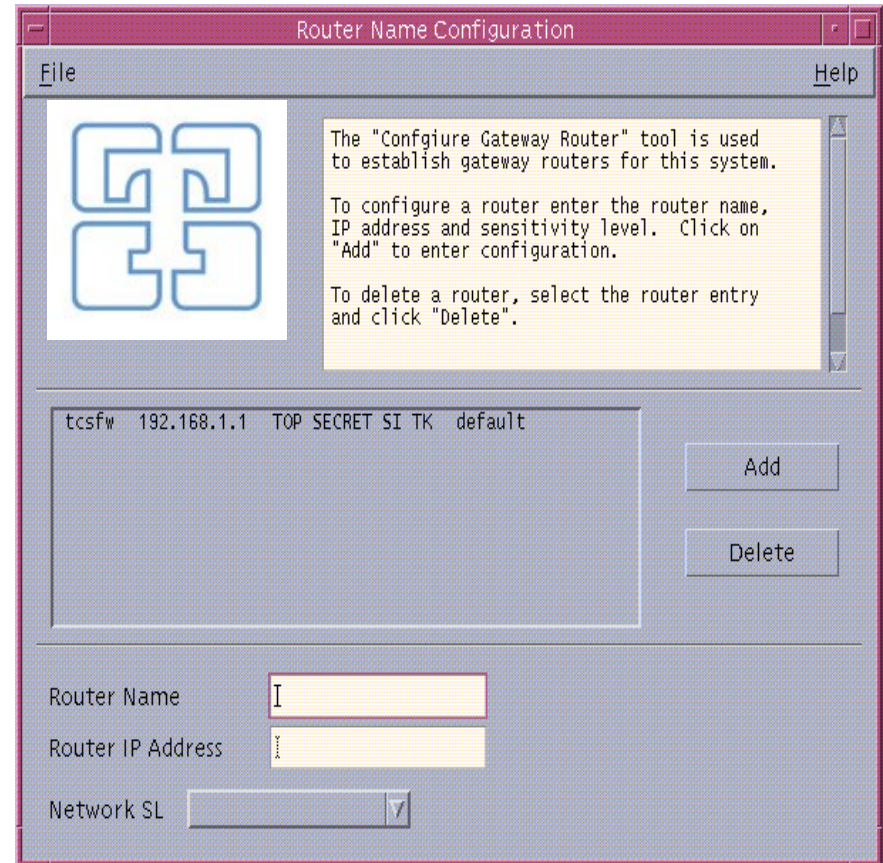
# SecureOffice TWS Administrator TCS System Administration Tools

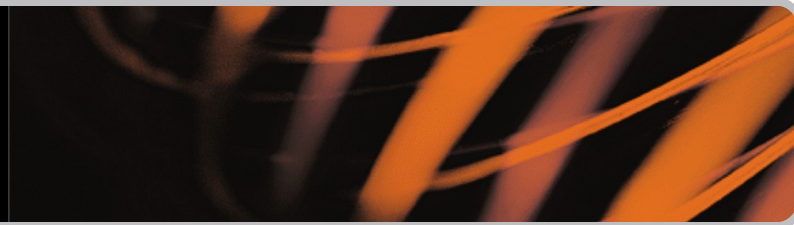
## Gateway Router Definition Tool



## Gateway Router Configuration Tool

- A gateway (border) router is needed to talk to hosts outside of the local network
- Sets up the gateway router to be the “default” route at each SL
- Each SL for each “System-High” network interface should have only one (1) default route.
- Allows “Trusted Routing” (via CIPSO labels)



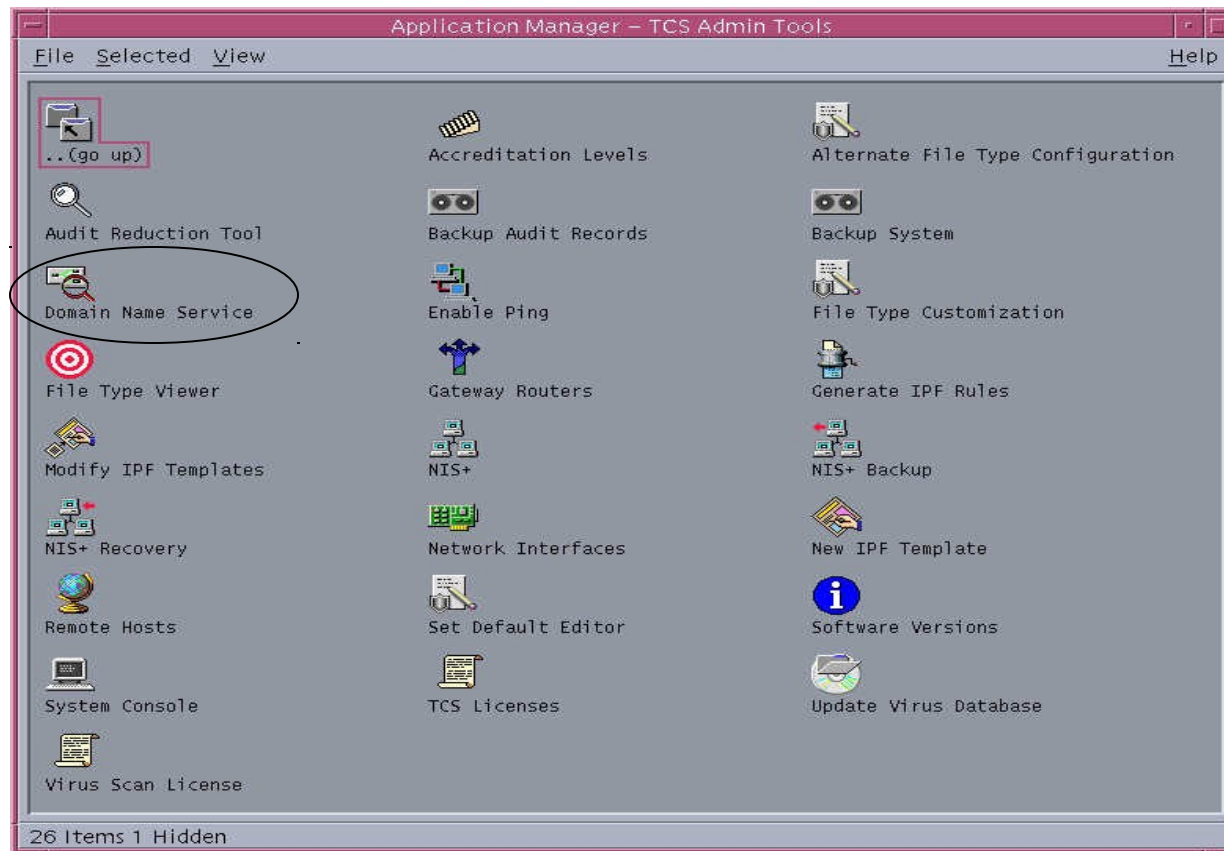


- Router Configuration Tool (con't)
  - **Router Name** - specify hostname associated with router interface on the same IP subnet.
  - **Router IP Address** - specify the IP address of the router interface on the same IP subnet.
  - **Network SL** - specify the "System-High" sensitivity label for the router interface on the same subnet. This should be the same as the network interface sensitivity label.

- Router Configuration Tool (con't)
  - **Add** Button - adds entry to tool list.
  - **Delete** Button - deletes highlighted entry in tool list.
  - **File** menu
    - **Save** - Save and configures current settings in tool
    - **Save and Exit** - Saves and configures current settings to system configuration and exits tool
    - **Exit** - Exits tool without saving changes.

# SecureOffice TWS Administrator TCS System Administration Tools

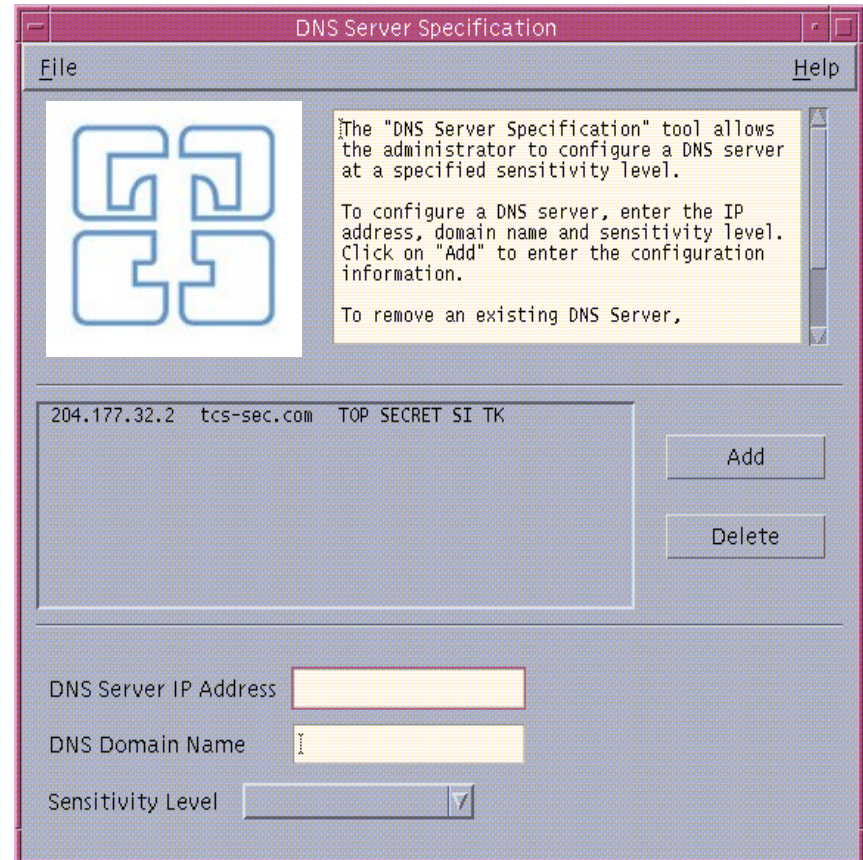
## Domain Name Service Definition Tool





## DNS Server Specification Tool

- DNS translates hostnames to IP addresses
- DNS client configuration only
- DNS Server is not configured on this machine
- Supports multiple DNS servers at each sensitivity label.





- DNS Server Specification Tool (con't)
  - **DNS Server IP Address** - IP address of the remote DNS server
  - **Default domain** - domain name value append to unqualified addresses
  - **Sensitivity Level** -sensitivity level of the remote DNS server.

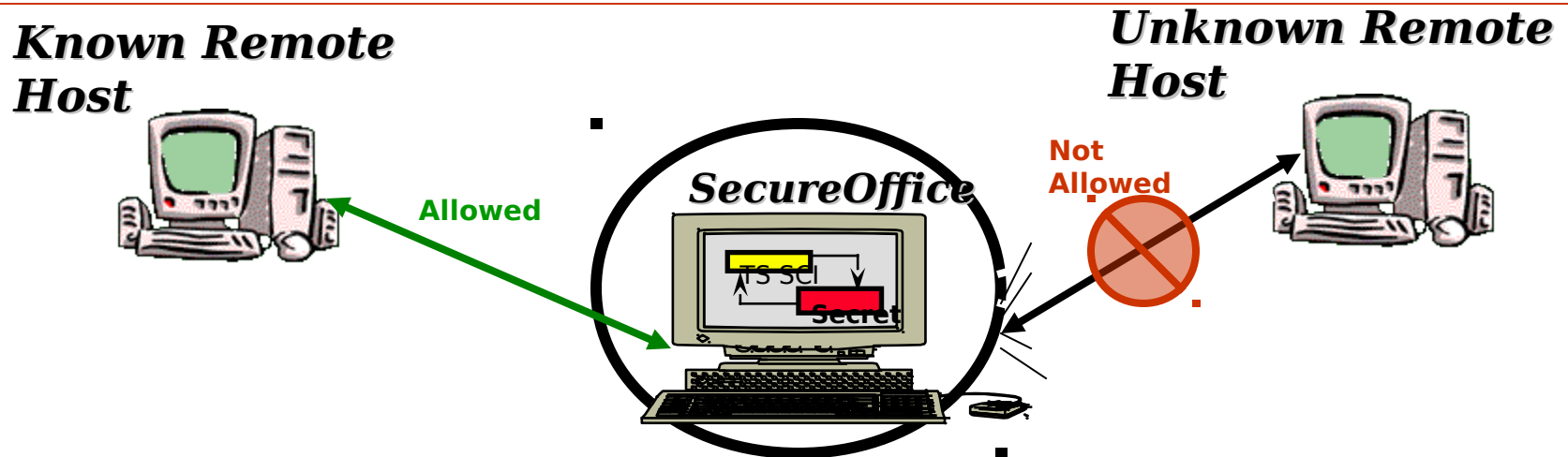
- DNS Server Specification Tool (con't)
  - **Add** Button - adds entry to tool list.
  - **Delete** Button - deletes highlighted entry in tool list.
  - **File** menu
    - **Save** - Save and configures current settings in tool
    - **Save and Exit** - Saves and configures current settings to system configuration and exits tool
    - **Exit** - Exits tool without saving changes.

# SecureOffice TWS

## Administrator

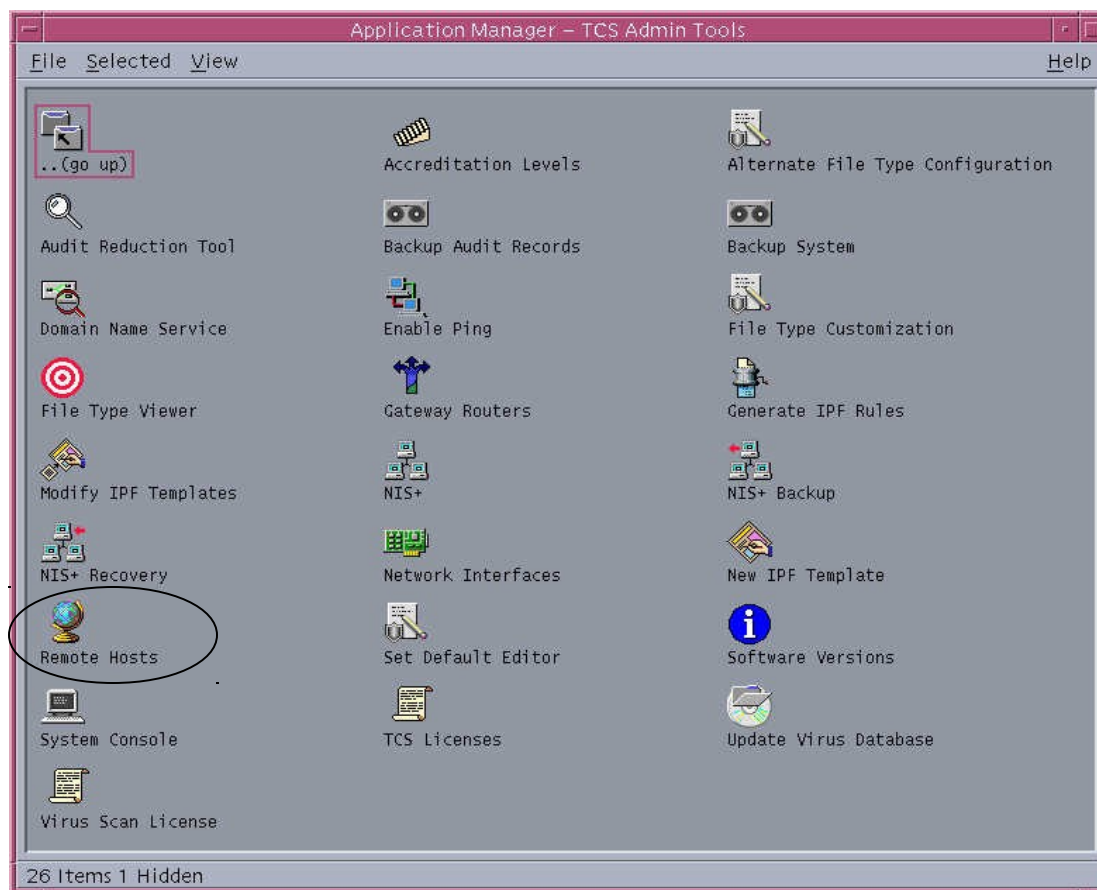
### TCS System Administration Tools

- Network Security Overview
  - Trusted network daemon (tnd) enforces MAC network security policy between SecureOffice workstation and all other remote hosts.
  - Trusted networking only allows communications between known defined remote hosts.
  - Host are “known” and defined in the Remote Hosts database using the TCS **Remote Host Tool**



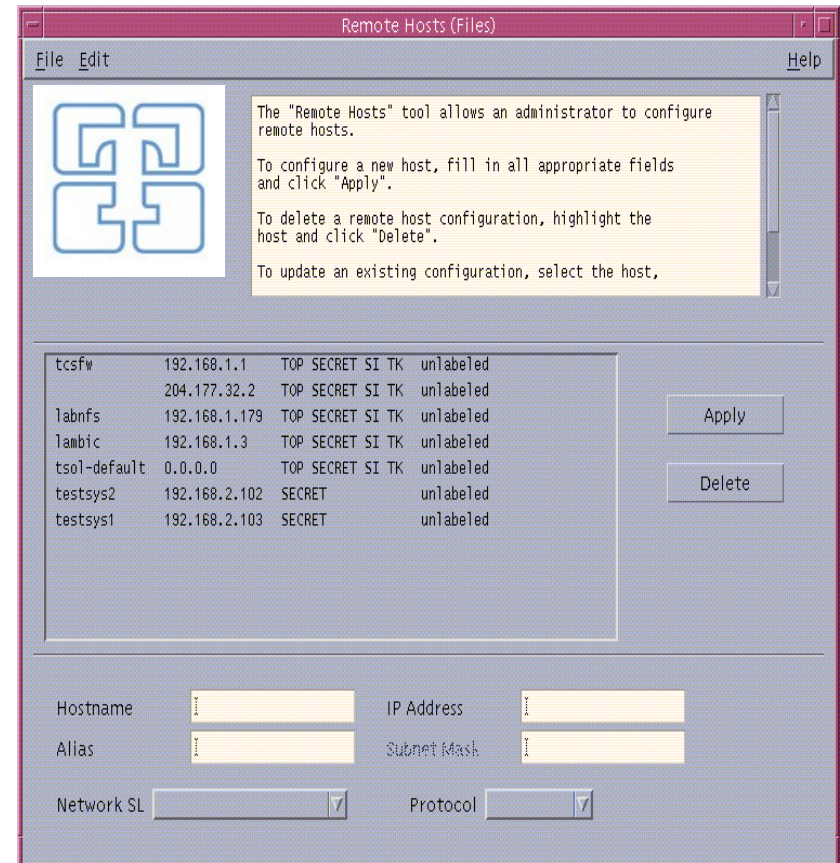
# SecureOffice TWS Administrator TCS System Administration Tools

## Remote Hosts Definition Tool



## Remote Host Tool

- Specify ALL remote hosts for network communication
- Excluding routers or DNS servers (added by Gateway and DNS tools)
- May specify multiple hosts or networks or sub networks with one entry -- "Wildcarding"



- Remote Host Tool (con't)
  - Remote Host IP Wildcards
    - Entry of individual hosts can become tiresome
    - You can define multiple host IPs with one entry
    - Each IP wildcard entry allows you to communicate with multiple hosts
    - All hosts in IP wildcard MUST be at the SAME Sensitivity Label (SL) and use the same prototype (labeled or unlabeled)
    - There must be commonalities in the IP addresses



## Remote Host IP Wildcard Examples

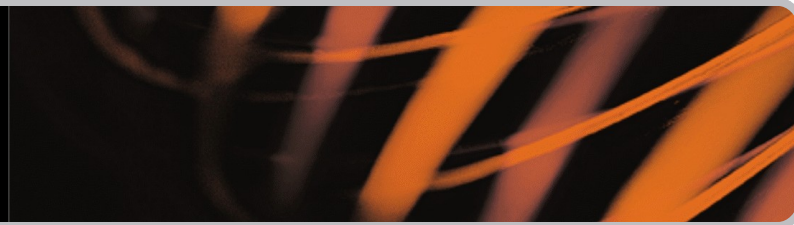
**X** - Represents a portion of the IP address

**0** - Represents the wildcard portion of the IP address

Wildcard	Description
<b>X.X.X.0</b>	Example: 192.168.1.0 represents IP addresses 192.168.1.1 to 192.168.1.254 (i.e., all IP addresses that begin with 192.168.1).
<b>X.X.0.0</b>	Example: 192.168.0.0 represents IP addresses 192.168.0.1 to 192.168.254.254 (i.e., all IP addresses that begin with 192.168).
<b>X.0.0.0</b>	Example: 192.0.0.0 represents IP addresses 192.0.0.1 to 192.254.254.254 (i.e., all IP addresses that begin with 192).
<b>0.0.0.0</b>	This is a special case that represents all IP addresses (i.e., the “allow all IP Addresses” wildcard). This entry allows communication with all IP addresses at the SL configured. This entry is typically configured for the network running at the highest SL allowed.

- Remote Host Tool (con't)
  - **Hostname**
    - Name of the remote host. When wildcards are used, this field can be used to identify the network (e.g. secret\_net) on which the remote hosts reside. Completing this field is optional.
  - **IP Address**
    - Address of the remote host in IP format X.X.X.X, where X is between 0 and 255. Completing this field is mandatory.
  - **Subnet Mask**
    - Completing this field is optional.
    - Entries in this field imply wildcarding. Do NOT use this field for normal individual host entries
  - **Alias**
    - Other names used to recognize a remote host. Completing this field is optional.

- Remote Host Tool (con't)
  - **Network SL**
    - Typically this is the “System High” network SL that the host resides on.
    - May also specify **Full Accreditation Range**
      - » Typically used for remote systems on the high side network interface that communicate with the Trusted Solaris labeled network security protocol.
    - Completing this field is mandatory.
  - **Protocol**
    - Unlabeled - used to indicate all other systems. It should be your choice unless you are certain that the host you are entering is running Trusted Solaris.
    - tsol - identifies another remote host running the Trusted Solaris labeled network security protocol.
    - Completing this field is mandatory.

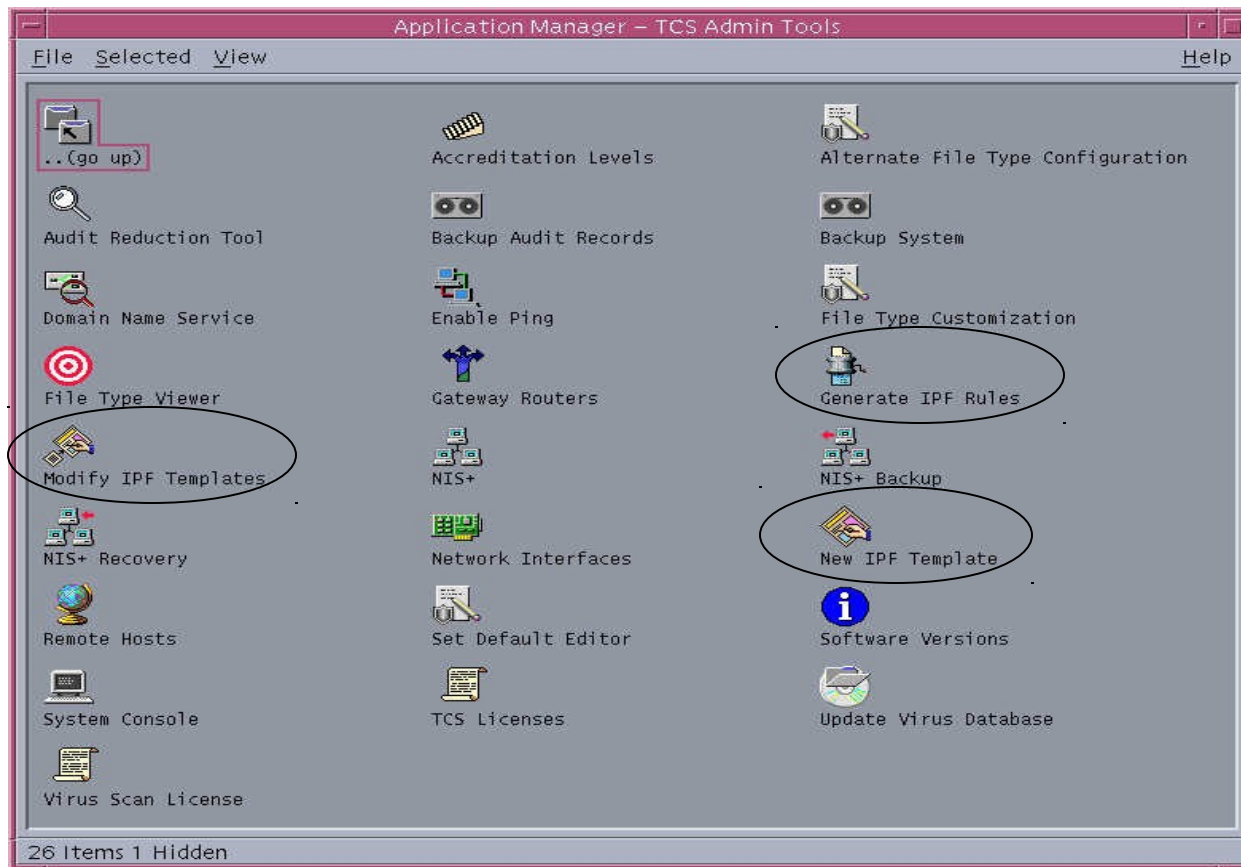


- Remote Host Tool (con't)
  - **Apply** Button - applies entries from tool list. Includes automatically generating and updating the IP filters.
  - **Delete** Button - deletes highlighted entry in tool list.
  - **File** menu
    - **Save** - Saves and configures current settings in tool
    - **Save and Exit** - Saves and configures current settings to system configuration and exits tool
    - **Exit** - Exits tool without saving and configuring changes.

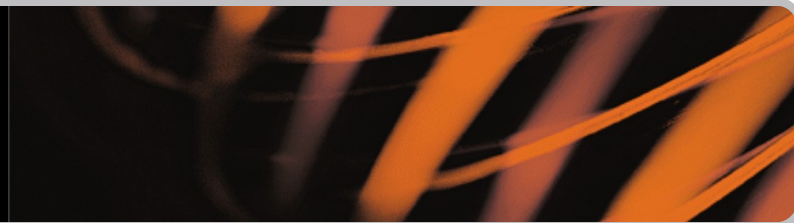
- Remote Host Tool (con't)
  - Edit Menu
    - **Copy**
      - » Makes a copy of the currently selected host or wildcard configuration for modification.
      - » Useful when adding a host or wildcard entry that is similar to an already existing host or wildcard entry.
    - **Retain Values**
      - » Maintains configuration information between new entries.
      - » Useful when a large number of hosts or wildcards are being added that are similar in their configuration.

# SecureOffice TWS Administrator TCS System Administration Tools

## IP Filtering Admin Tools



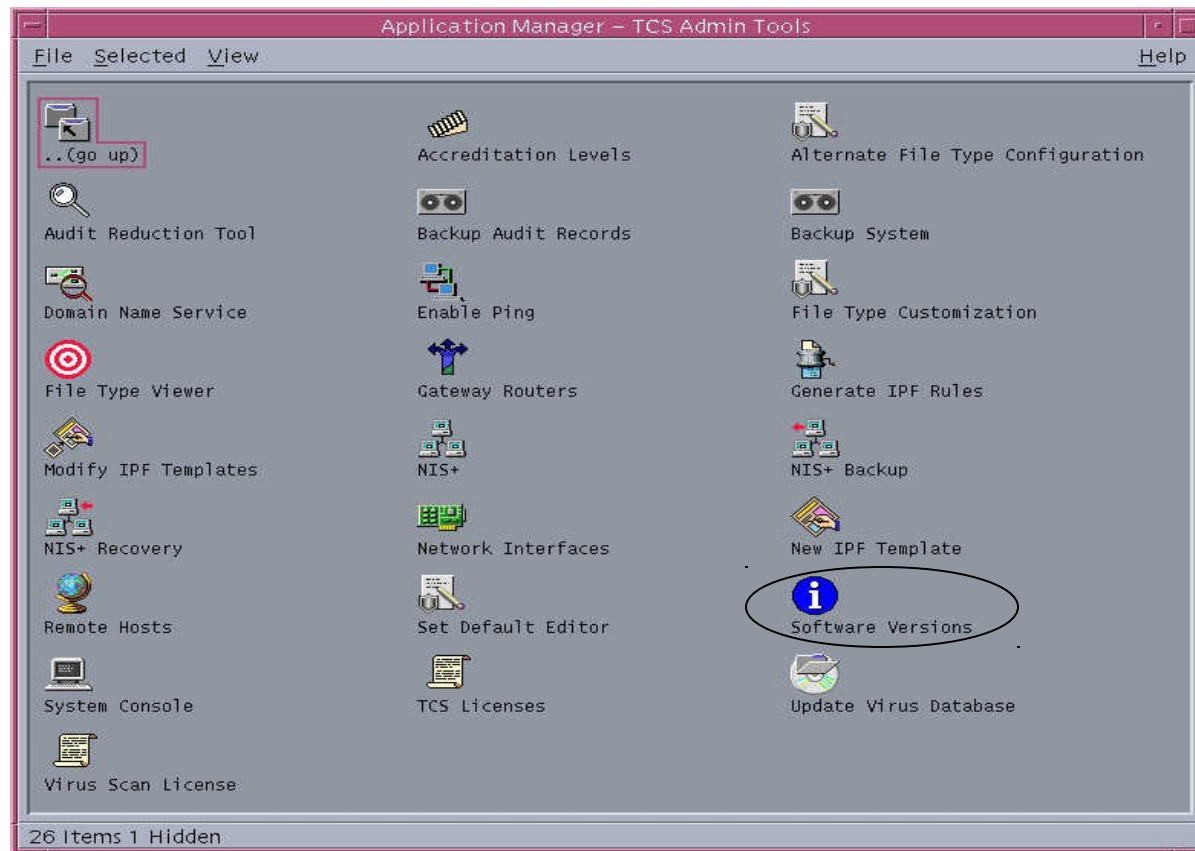




- IP Filtering Admin Tools
  - Generate IPF Rules
    - Action used to create new IP filtering rules
    - Creates `/etc/opt/ipf/ipf.conf` from all templates
    - This will not only create the rules but it also loads them
  - Modify IPF Template
    - Utility used to edit an existing IP filtering template
  - New IPF Template
    - Utility used to create an interface specific IP filtering template

# SecureOffice TWS Administrator TCS System Administration Tools

## Software Version Description Tool

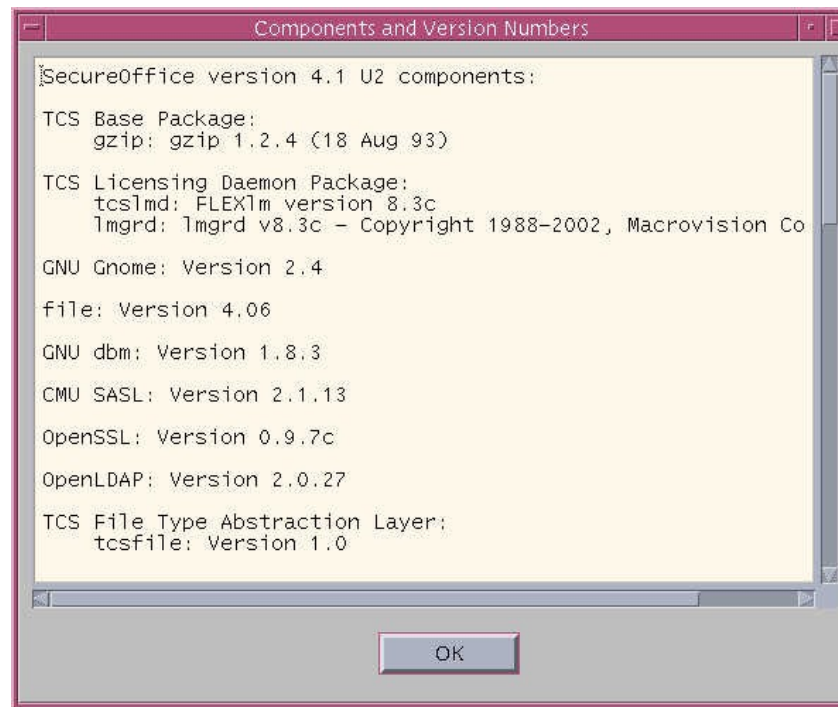


# SecureOffice TWS

## Administrator

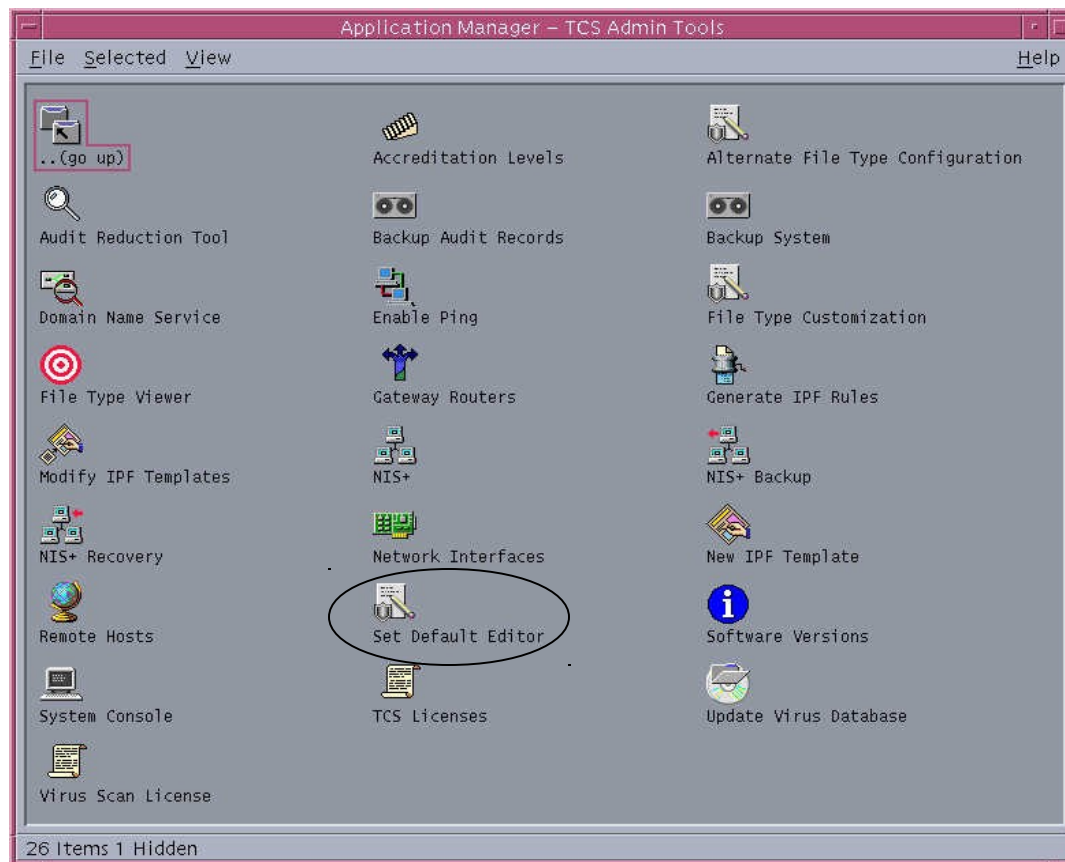
### TCS System Administration Tools

- View Software Versions
  - Defines version information for all software products (including 3rd Party) installed with TWS



# SecureOffice TWS Administrator TCS System Administration Tools

## Set Default Editor Tool



- Set Default Editor
  - Allows administrator to define the desired editor for command line based configuration tools



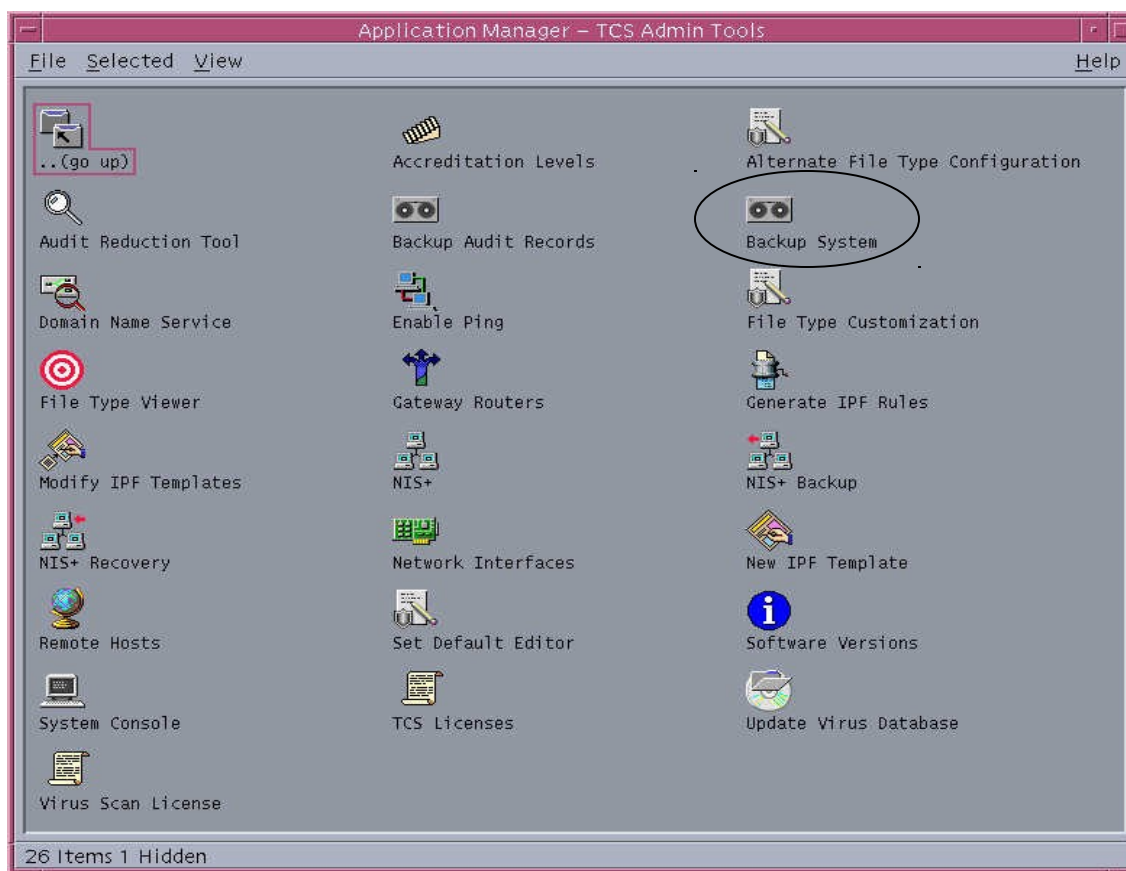
- Set Default Editor, cont.





# SecureOffice TWS Administrator TCS System Administration Tools

## System Backup Tool

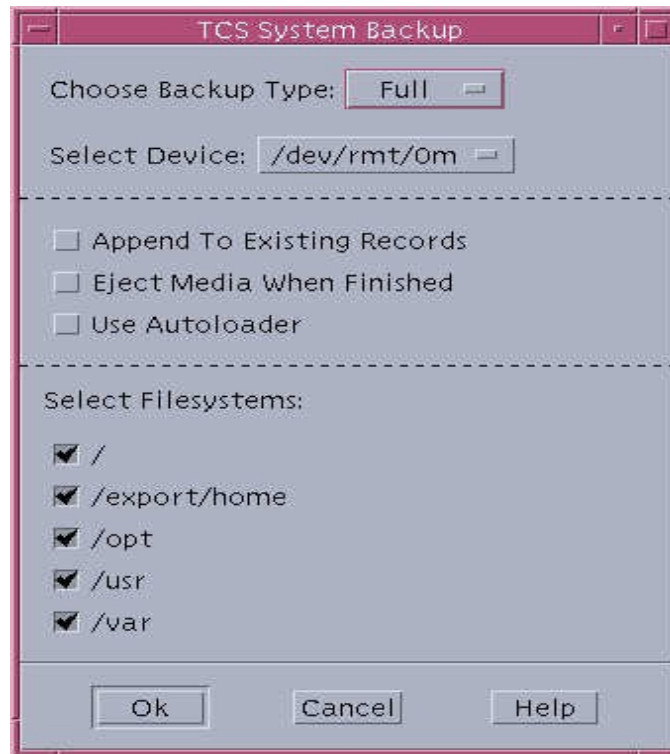


# SecureOffice TWS

## Administrator

### TCS System Administration Tools

- System Backup Tool
  - Provides definition fields for conducting system backups



# SecureOffice TWS

## Administrator

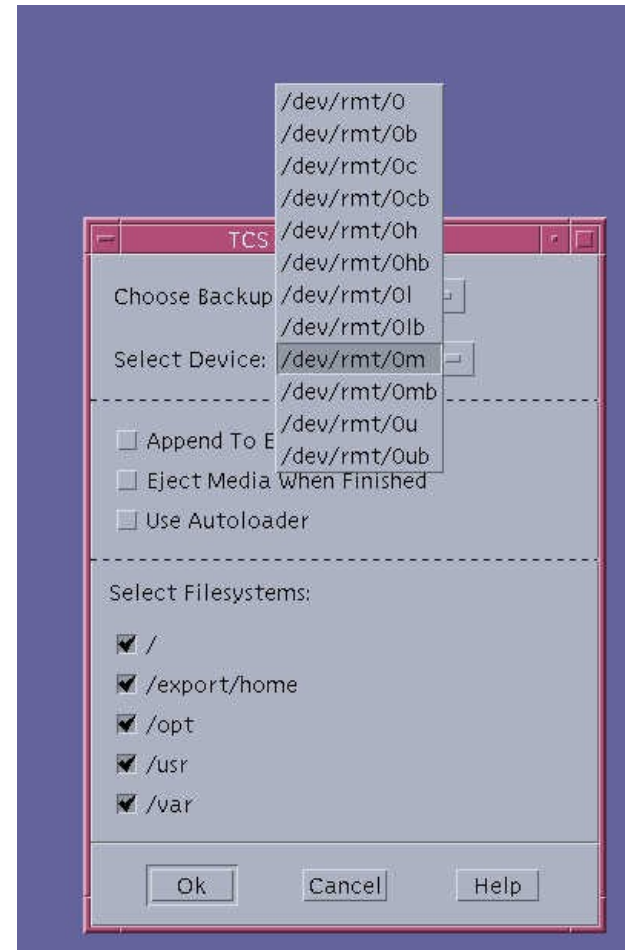
### TCS System Administration Tools

- System Backup Tool
  - Select Backup Level
    - Full
    - Weekly
    - Daily

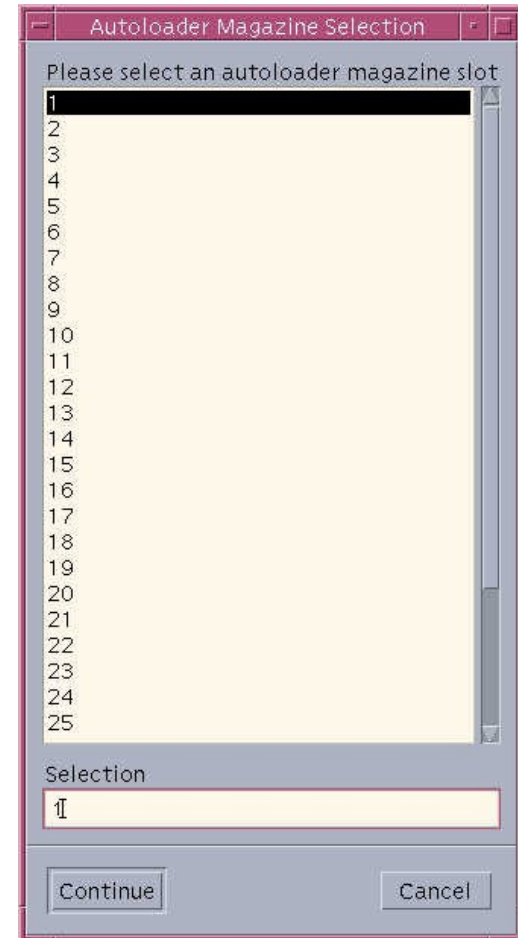


# SecureOffice TWS Administrator TCS System Administration Tools

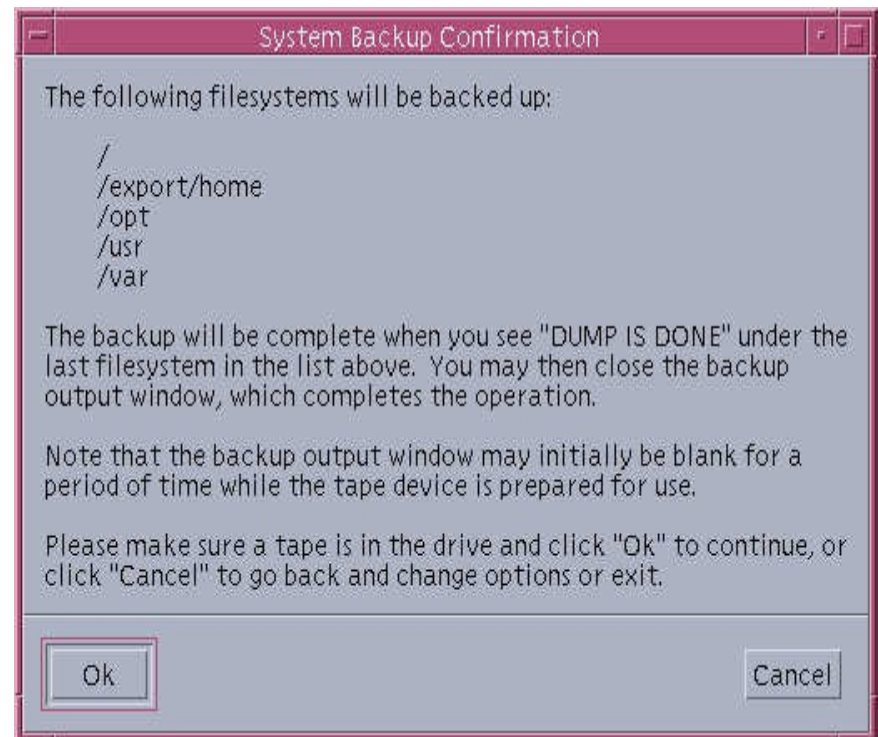
- System Backup Tool
  - Select Tape Device
    - Specify appropriate tape device



- System Backup Tool
  - Select Autoloader Tape Slot
    - Allows administrator to manually select the autoloader tape slot to use for backup



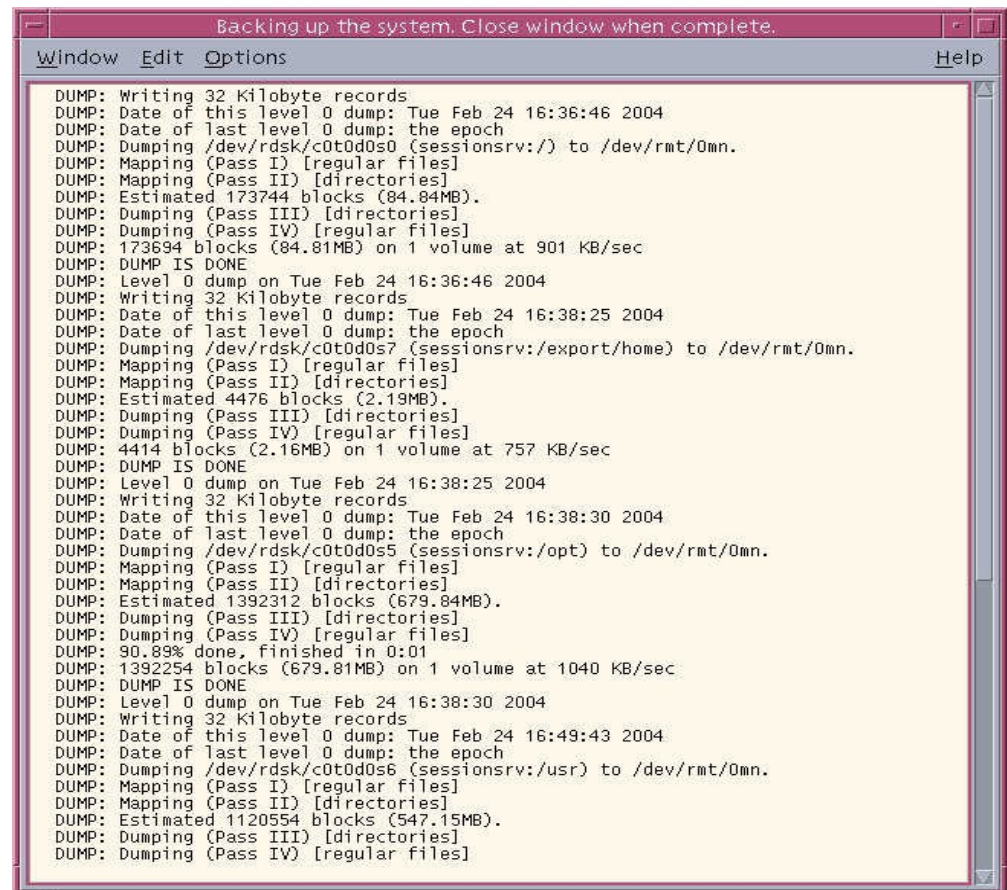
- System Backup Tool
  - Confirmation Window
    - Provides administrator feedback on the backup operation





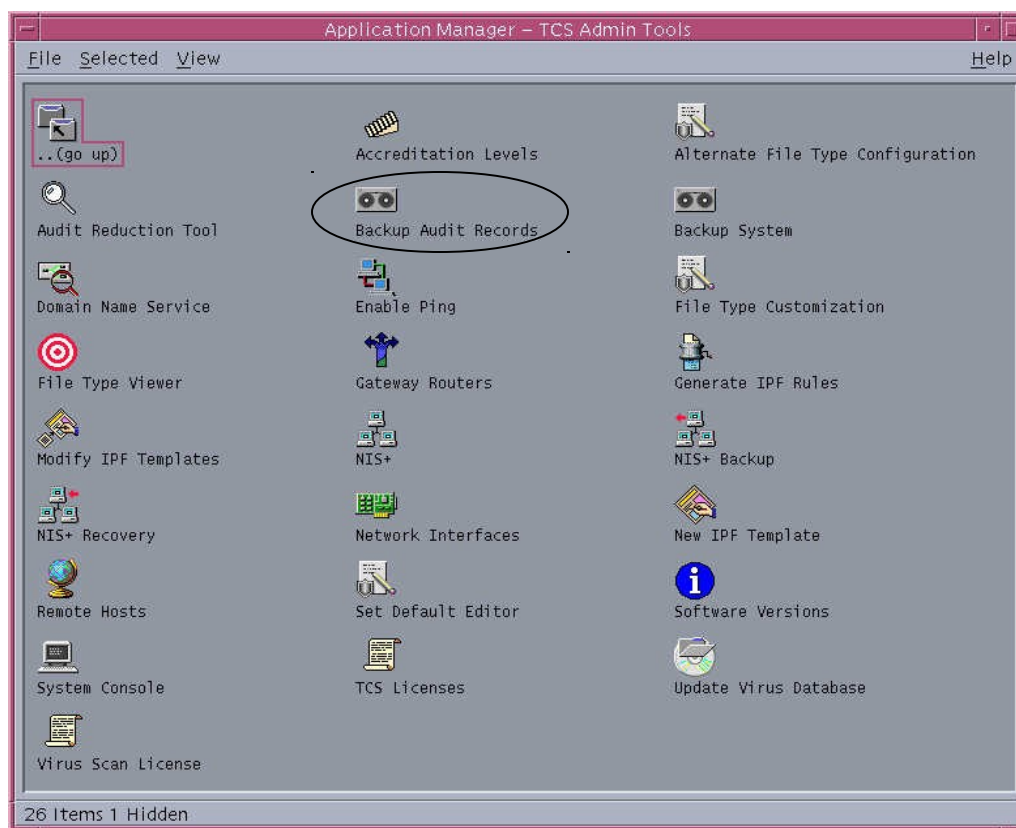
# SecureOffice TWS Administrator TCS System Administration Tools

- System Backup Tool
  - Backup Output

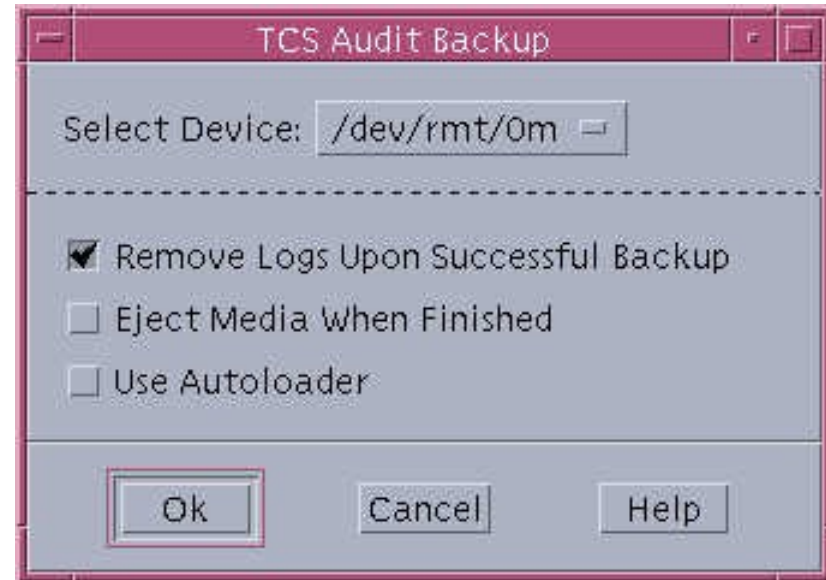


```
Window Edit Options Help
DUMP: Writing 32 Kilobyte records
DUMP: Date of this level 0 dump: Tue Feb 24 16:36:46 2004
DUMP: Date of last level 0 dump: the epoch
DUMP: Dumping /dev/rdsk/c0t0d0s0 (sessionsrv:/) to /dev/rmt/0mn.
DUMP: Mapping (Pass I) [regular files]
DUMP: Mapping (Pass II) [directories]
DUMP: Estimated 173744 blocks (84.84MB).
DUMP: Dumping (Pass III) [directories]
DUMP: Dumping (Pass IV) [regular files]
DUMP: 173694 blocks (84.81MB) on 1 volume at 901 KB/sec
DUMP: DUMP IS DONE
DUMP: Level 0 dump on Tue Feb 24 16:36:46 2004
DUMP: Writing 32 Kilobyte records
DUMP: Date of this level 0 dump: Tue Feb 24 16:38:25 2004
DUMP: Date of last level 0 dump: the epoch
DUMP: Dumping /dev/rdsk/c0t0d0s7 (sessionsrv:/export/home) to /dev/rmt/0mn.
DUMP: Mapping (Pass I) [regular files]
DUMP: Mapping (Pass II) [directories]
DUMP: Estimated 4476 blocks (2.19MB).
DUMP: Dumping (Pass III) [directories]
DUMP: Dumping (Pass IV) [regular files]
DUMP: 4414 blocks (2.16MB) on 1 volume at 757 KB/sec
DUMP: DUMP IS DONE
DUMP: Level 0 dump on Tue Feb 24 16:38:25 2004
DUMP: Writing 32 Kilobyte records
DUMP: Date of this level 0 dump: Tue Feb 24 16:38:30 2004
DUMP: Date of last level 0 dump: the epoch
DUMP: Dumping /dev/rdsk/c0t0d0s5 (sessionsrv:/opt) to /dev/rmt/0mn.
DUMP: Mapping (Pass I) [regular files]
DUMP: Mapping (Pass II) [directories]
DUMP: Estimated 1392312 blocks (679.84MB).
DUMP: Dumping (Pass III) [directories]
DUMP: Dumping (Pass IV) [regular files]
DUMP: 90.89% done, finished in 0:01
DUMP: 1392254 blocks (679.81MB) on 1 volume at 1040 KB/sec
DUMP: DUMP IS DONE
DUMP: Level 0 dump on Tue Feb 24 16:38:30 2004
DUMP: Writing 32 Kilobyte records
DUMP: Date of this level 0 dump: Tue Feb 24 16:49:43 2004
DUMP: Date of last level 0 dump: the epoch
DUMP: Dumping /dev/rdsk/c0t0d0s6 (sessionsrv:/usr) to /dev/rmt/0mn.
DUMP: Mapping (Pass I) [regular files]
DUMP: Mapping (Pass II) [directories]
DUMP: Estimated 1120554 blocks (547.15MB).
DUMP: Dumping (Pass III) [directories]
DUMP: Dumping (Pass IV) [regular files]
```

## Audit Backup Tool



- Audit Backup Tool
  - Allows administrator to define the audit backup operation

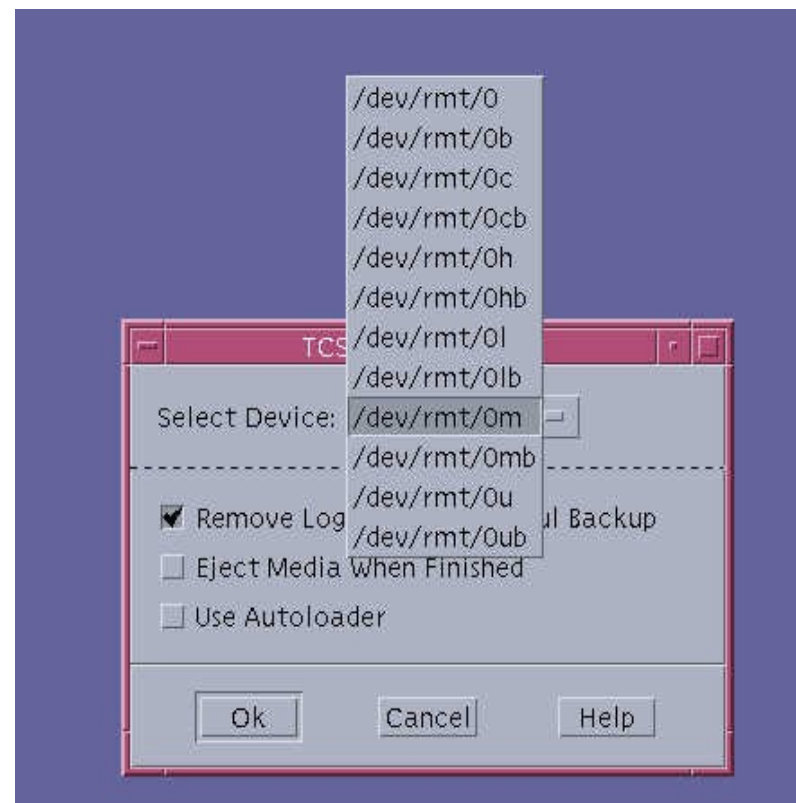


# SecureOffice TWS

## Administrator

### TCS System Administration Tools

- Audit Backup Tool
  - Tape Device Selection
    - Administrator selects appropriate tape device for audit backup



- Audit Backup Tool
  - No Device Found Error
    - Occurs when no tape device is accessible by the system



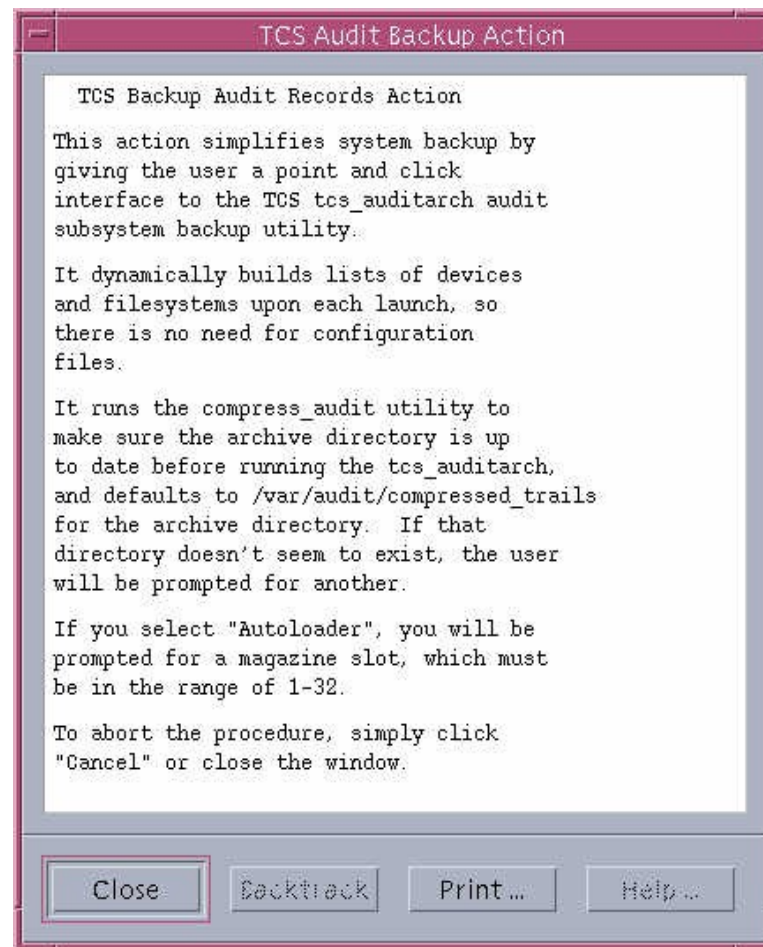


# SecureOffice TWS

## Administrator

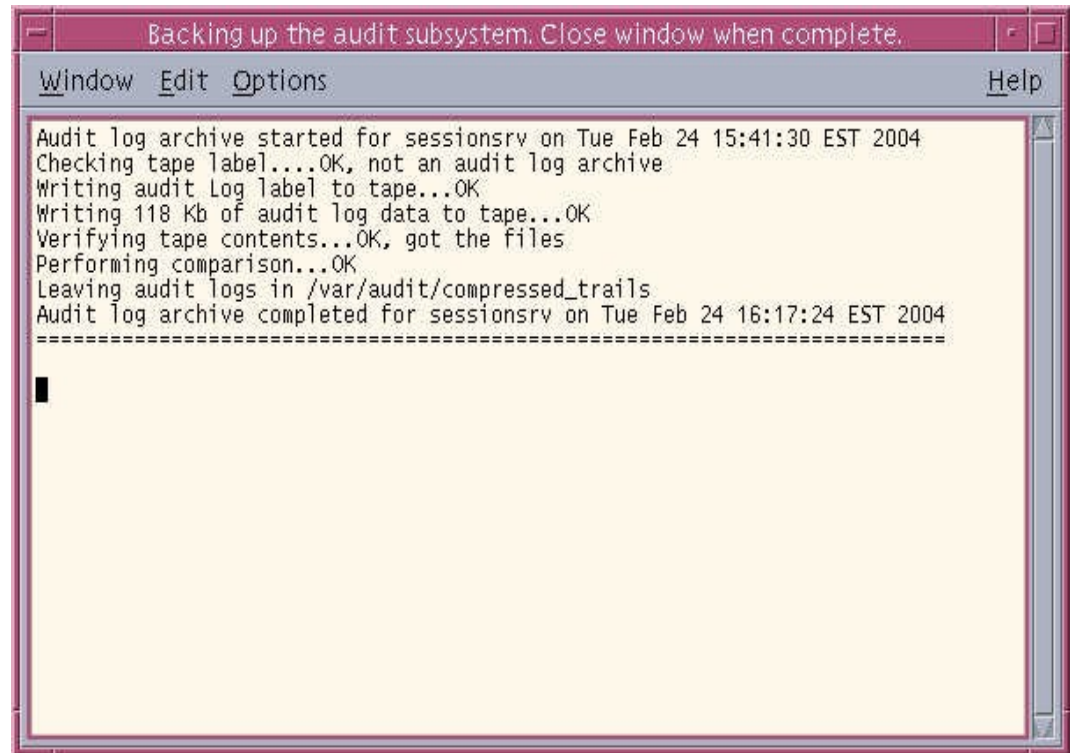
### TCS System Administration Tools

- Audit Backup Tool
  - Help Screen





- Audit Backup Tool
  - Completion Dialog



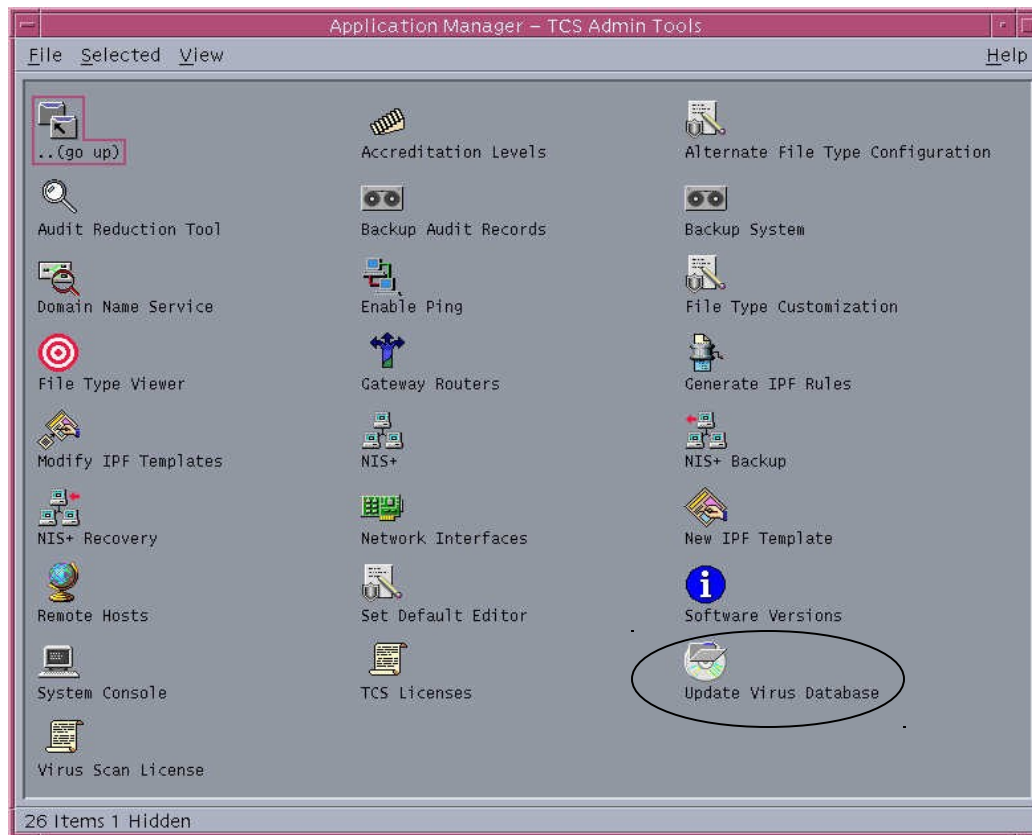
The screenshot shows a window titled "Backing up the audit subsystem: Close window when complete." with a menu bar containing "Window", "Edit", "Options", and "Help". The main text area displays the following log:

```
Audit log archive started for sessionsrv on Tue Feb 24 15:41:30 EST 2004
Checking tape label....OK, not an audit log archive
Writing audit Log label to tape...OK
Writing 118 Kb of audit log data to tape...OK
Verifying tape contents...OK, got the files
Performing comparison...OK
Leaving audit logs in /var/audit/compressed_trails
Audit log archive completed for sessionsrv on Tue Feb 24 16:17:24 EST 2004
=====
```

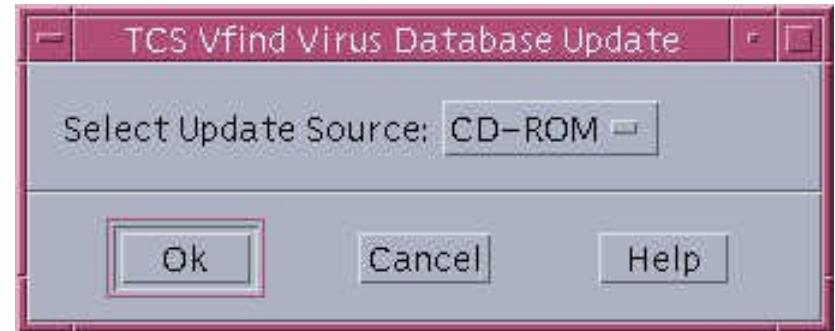
A cursor is visible at the bottom left of the text area.

# SecureOffice TWS Administrator TCS System Administration Tools

## VFind Virus Definition List Update Tool



- VFind Virus Definition List Update
  - Allows administrator to easily update Virus Definition Lists (VDL's)

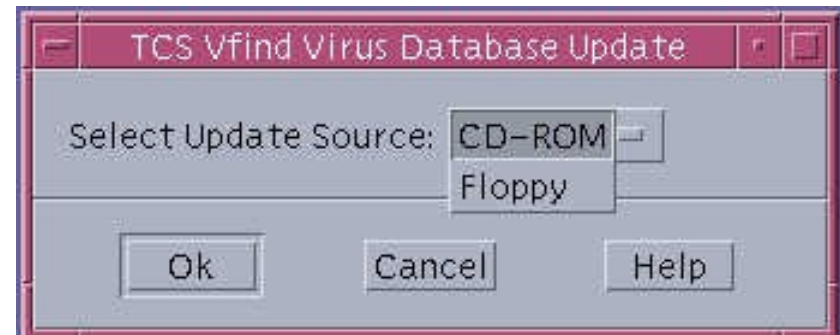


# SecureOffice TWS

## Administrator

### TCS System Administration Tools

- VFind VDL Update Tool
  - Media Selection
    - Select appropriate media for VDL upload

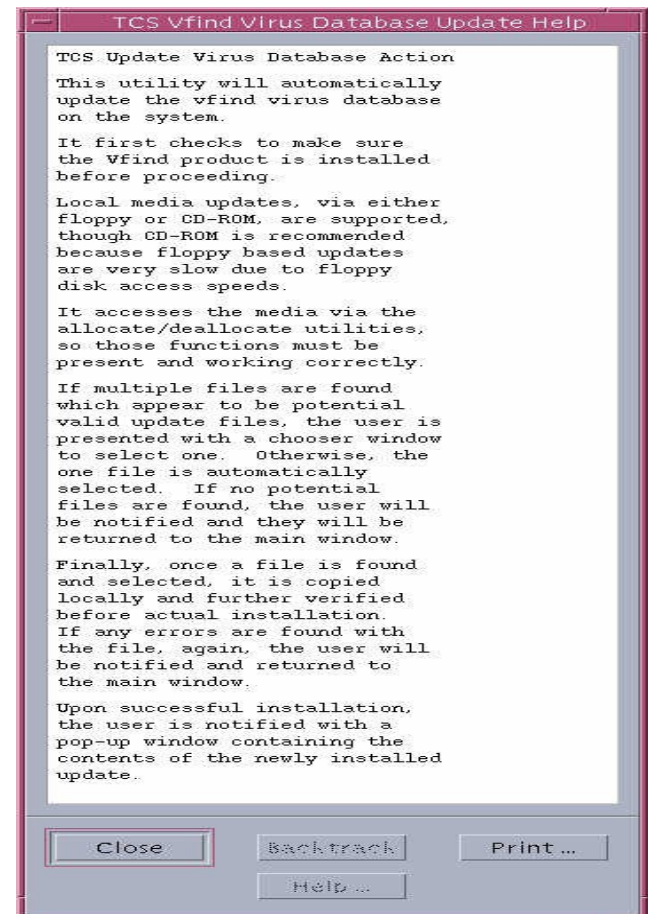


# SecureOffice TWS

## Administrator

### TCS System Administration Tools

- VFind VDL Update Tool
  - Help Screen



# SecureOffice TWS

## Administrator

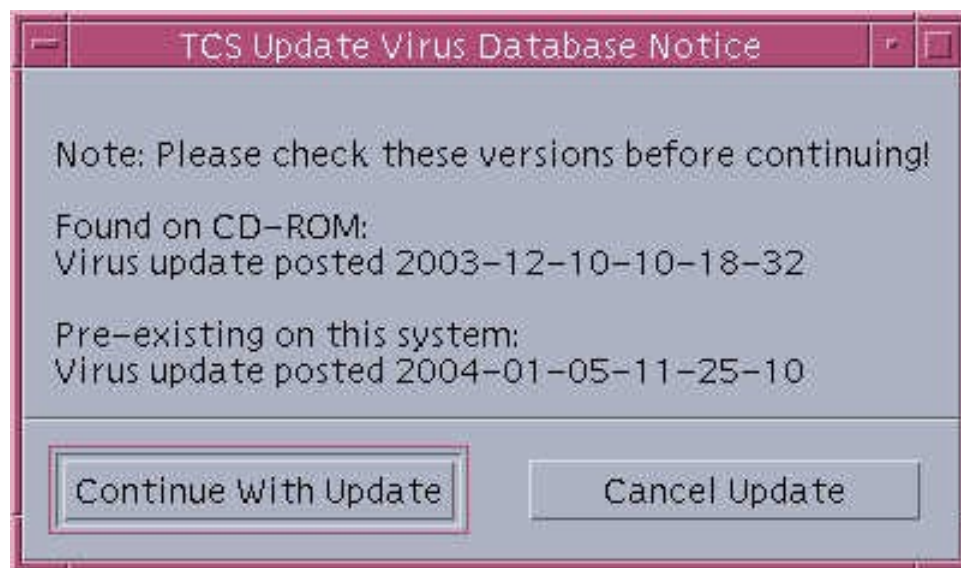
### TCS System Administration Tools

- VFind VDL Update Tool
  - Device allocation screens
  - Always select "Yes" to "Do you want cdrom\_0 mounted?"





- VFind VDL Update Tool
  - VDL update verification screen
  - If this data is correct, select "Continue With Update"

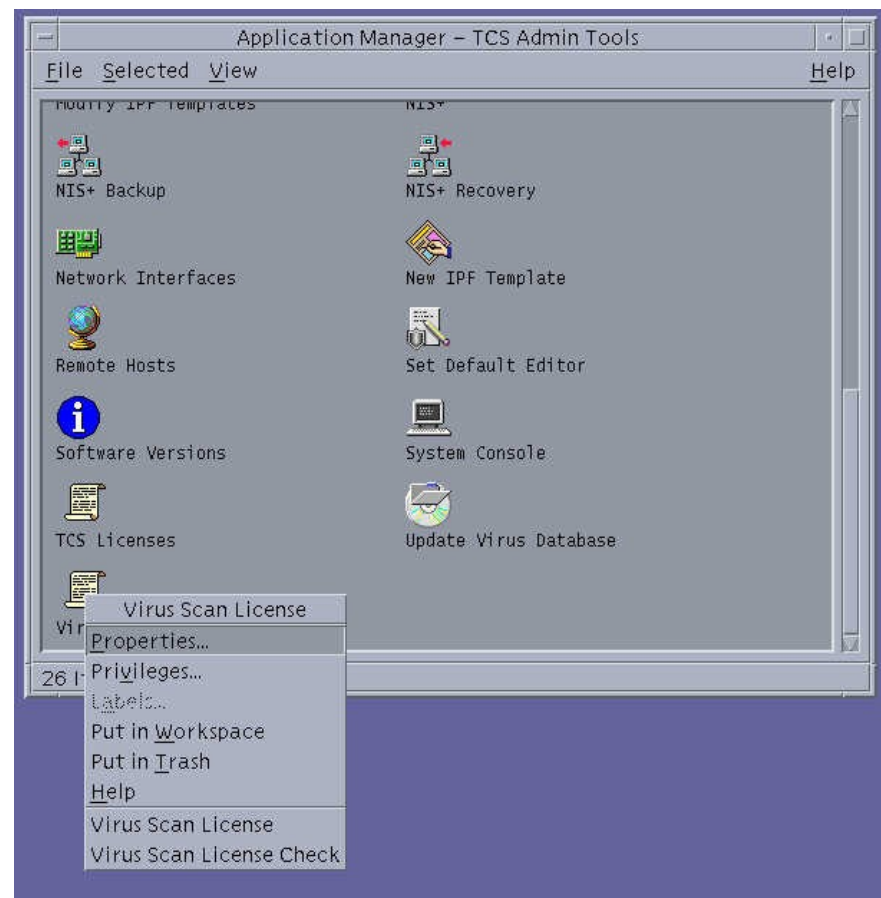


- VFind VDL Update Tool
  - VDL Update success dialog

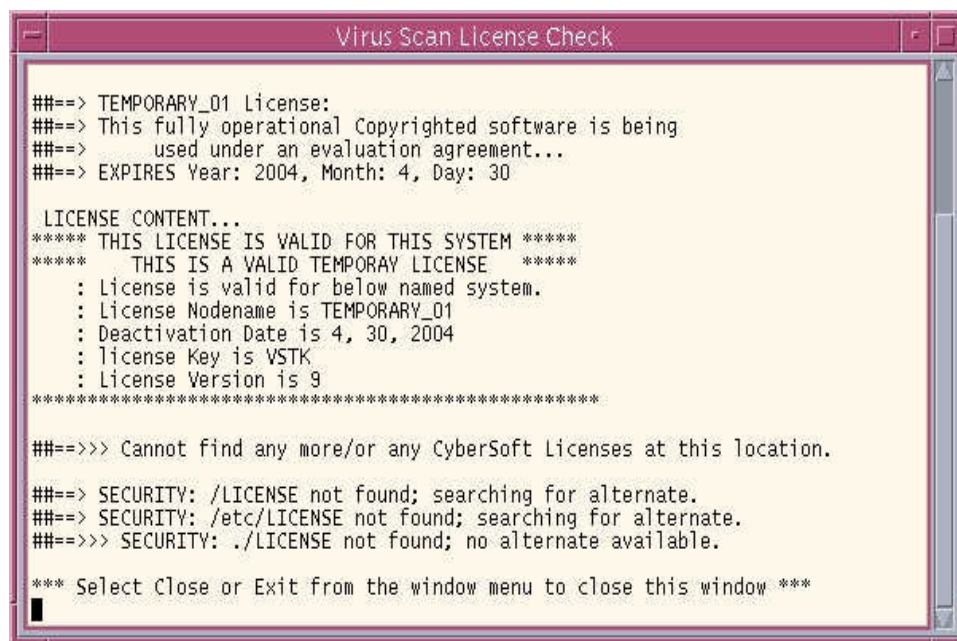


# SecureOffice TWS Administrator TCS System Administration Tools

- VFind License Verification
  - Verifies proper installation of VFind Virus Scan license
  - Right-click on Virus Scan License icon
  - Select Virus Scan License Check



- VFind License Verification
  - Displays the results of the VFind Virus Scan license check



```
Virus Scan License Check

##==> TEMPORARY_01 License:
##==> This fully operational Copyrighted software is being
##==>      used under an evaluation agreement...
##==> EXPIRES Year: 2004, Month: 4, Day: 30

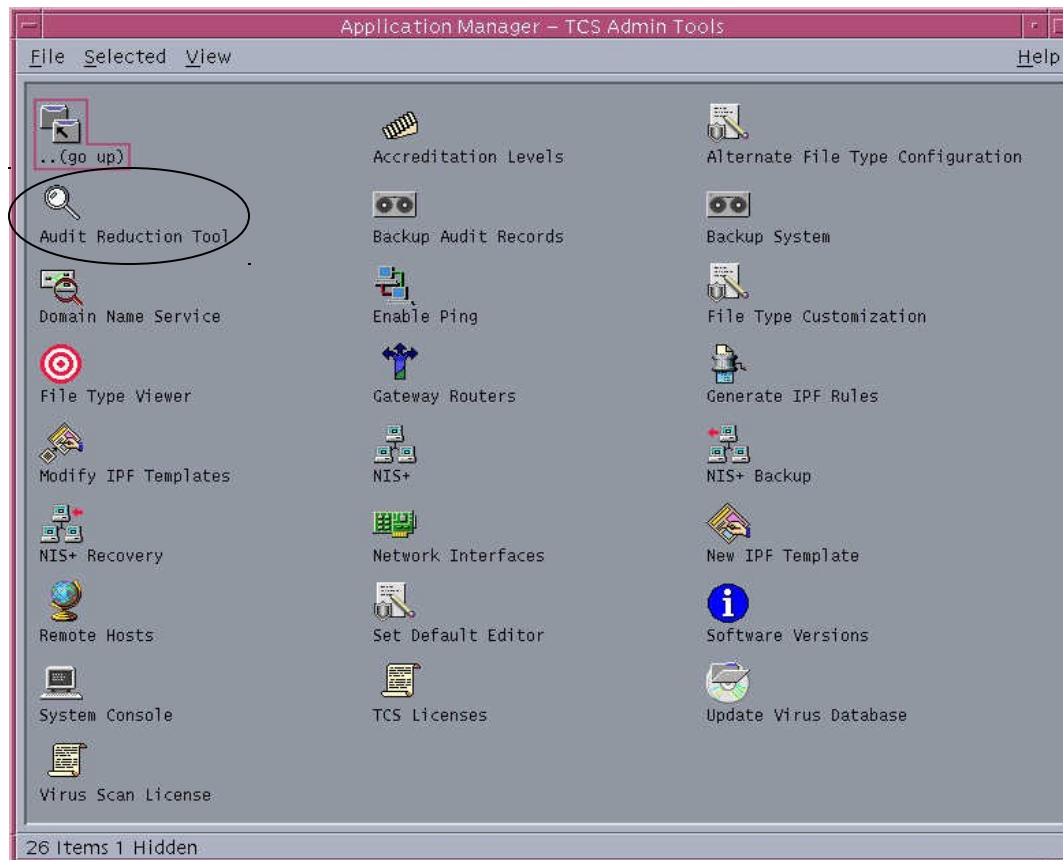
LICENSE CONTENT...
**** THIS LICENSE IS VALID FOR THIS SYSTEM ****
****   THIS IS A VALID TEMPORAY LICENSE   ****
: License is valid for below named system.
: License Nodename is TEMPORARY_01
: Deactivation Date is 4, 30, 2004
: license Key is VSTK
: License Version is 9
*****

##==>>> Cannot find any more/or any CyberSoft Licenses at this location.

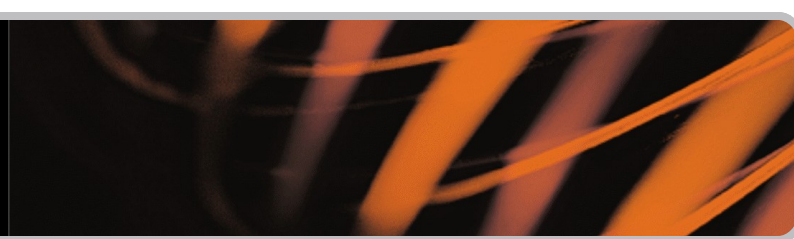
##==> SECURITY: /LICENSE not found; searching for alternate.
##==> SECURITY: /etc/LICENSE not found; searching for alternate.
##==>>> SECURITY: ./LICENSE not found; no alternate available.

*** Select Close or Exit from the window menu to close this window ***
```

## Audit Reduction Tool



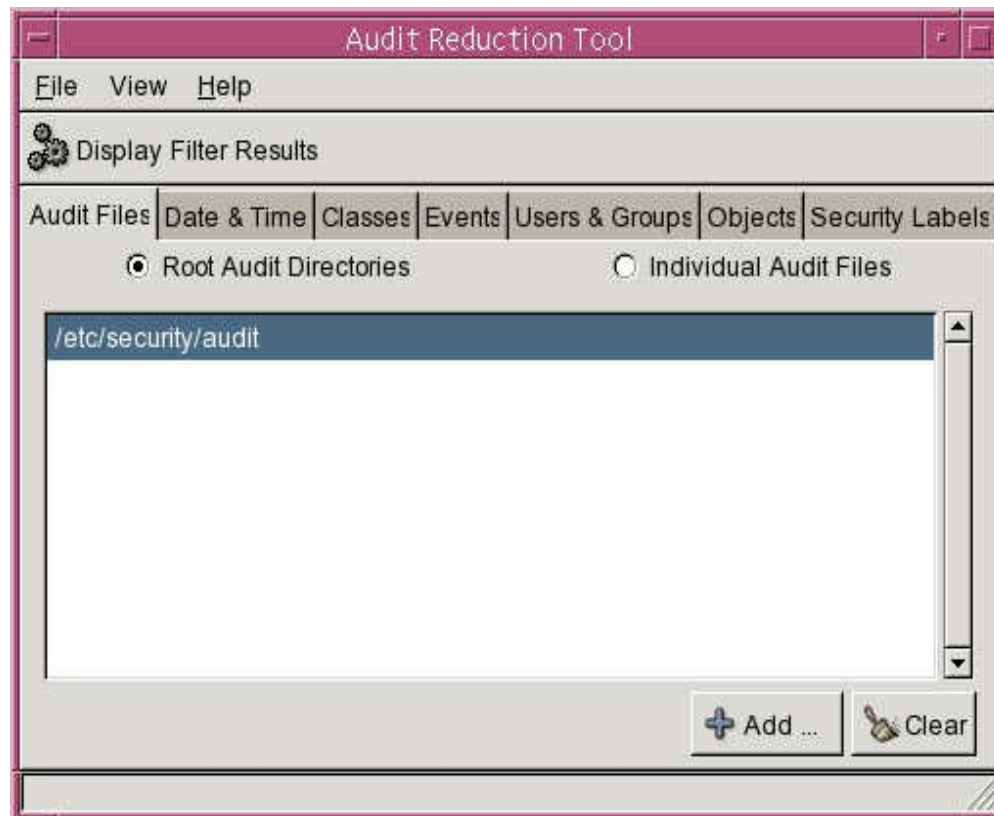




- Audit Reduction Tool
  - Allows administrators to review audit data
  - Provides selection criteria
    - Date & Time
    - Audit Classes
    - Audit Events
    - Users & Groups
    - Objects (Files)
    - Security Level(s)

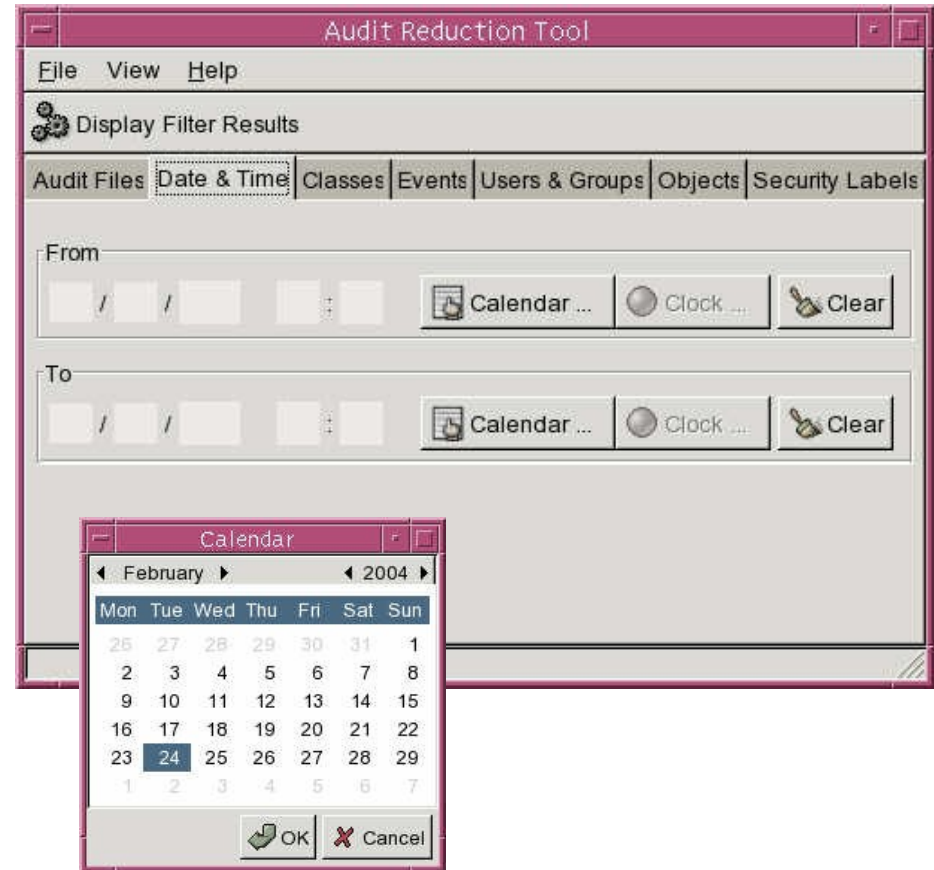


- Audit Reduction Tool
  - Main Window
  - Select audit directories/files to review



# SecureOffice TWS Administrator TCS System Administration Tools

- Audit Reduction Tool
  - Date & Time Selection
  - Use Calendar function to easily select date or date range for review
  - Use Clock function to select time or range of times for review

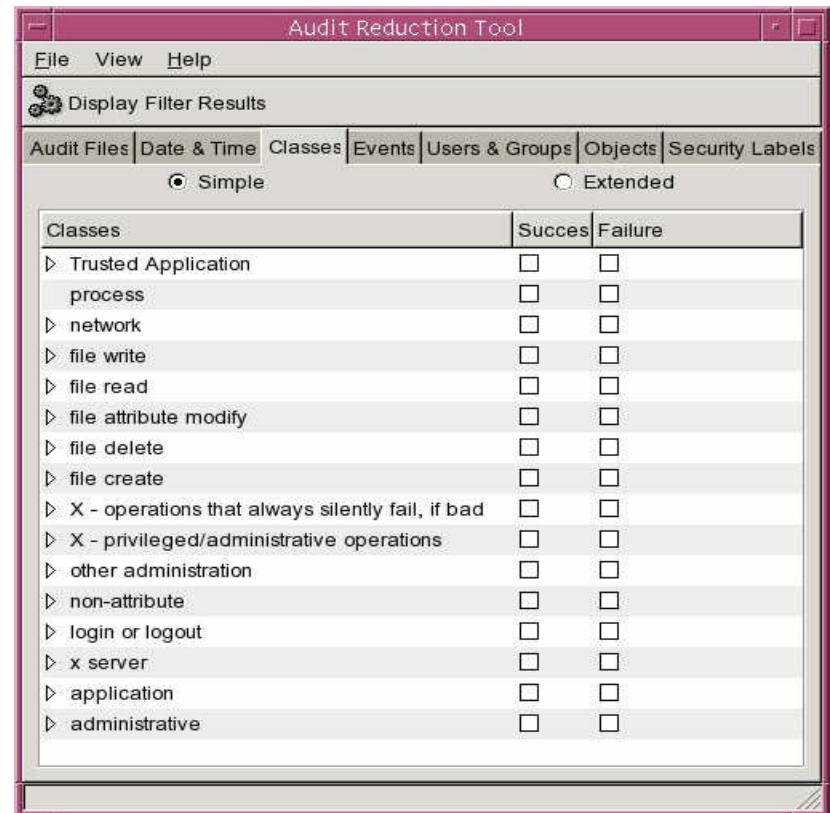


# SecureOffice TWS

## Administrator

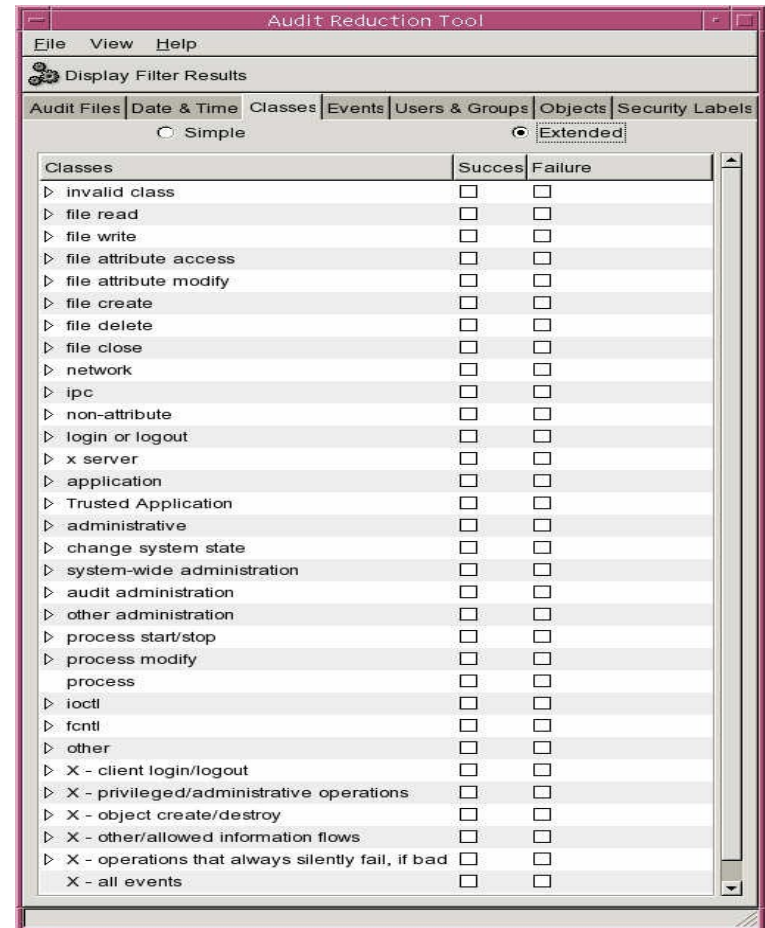
### TCS System Administration Tools

- Audit Reduction Tool
  - Audit Class Selection
    - Select from Simple or Extended Audit Class lists
    - Select Successes, Failures, or both



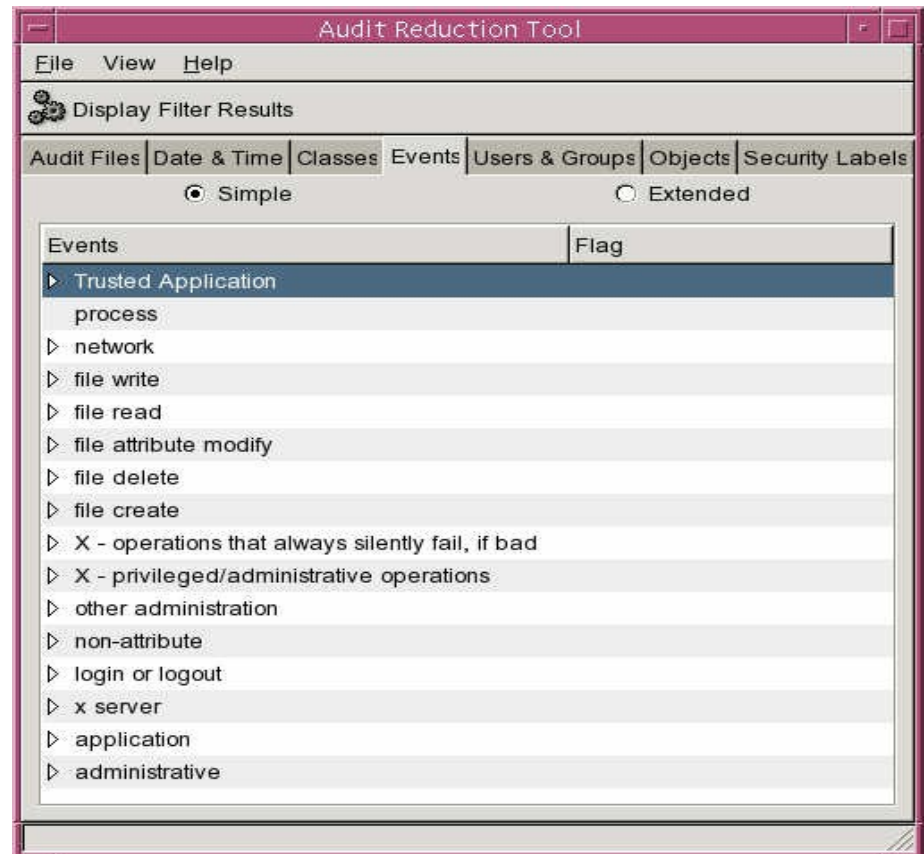
# SecureOffice TWS Administrator TCS System Administration Tools

- Audit Reduction Tool
  - Extended Audit Class list



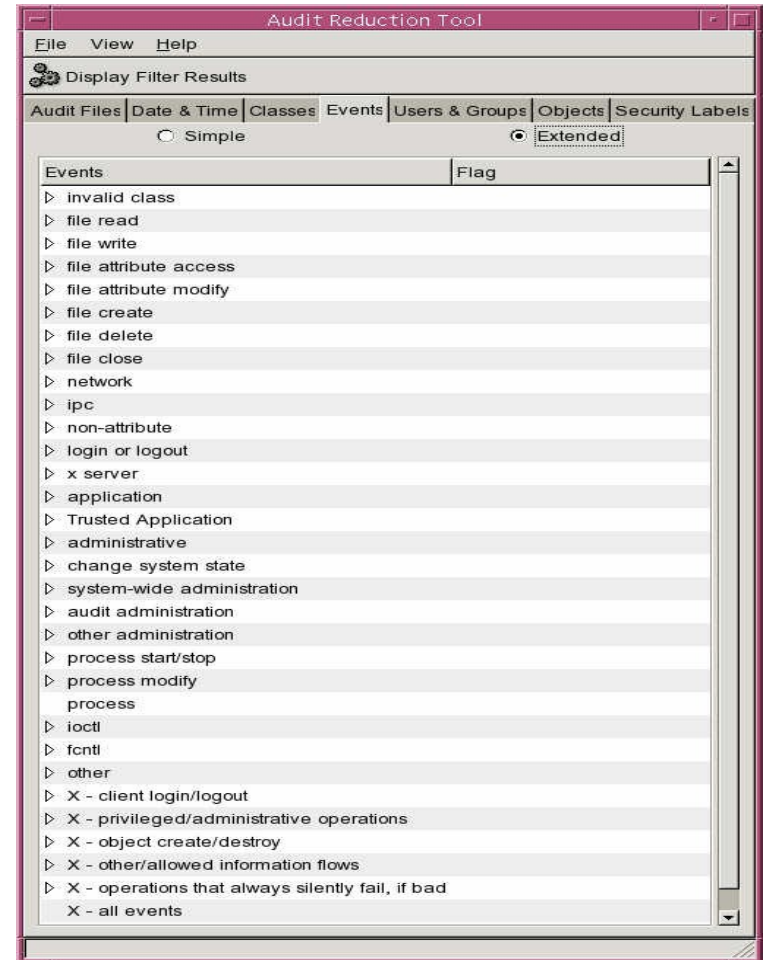
# SecureOffice TWS Administrator TCS System Administration Tools

- Audit Reduction Tool
  - Audit Event Selection
    - Select from Simple or Extended Audit Event lists
    - Select Successes, Failures, or both



# SecureOffice TWS Administrator TCS System Administration Tools

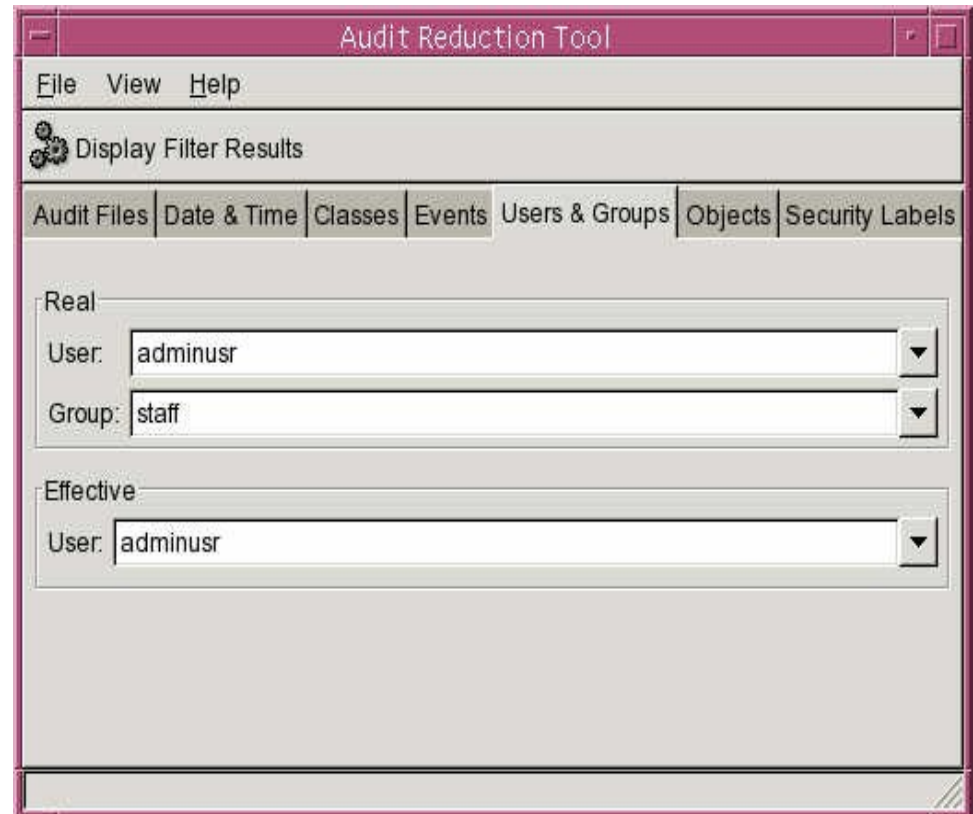
- Audit Reduction Tool
  - Extended Audit Event list



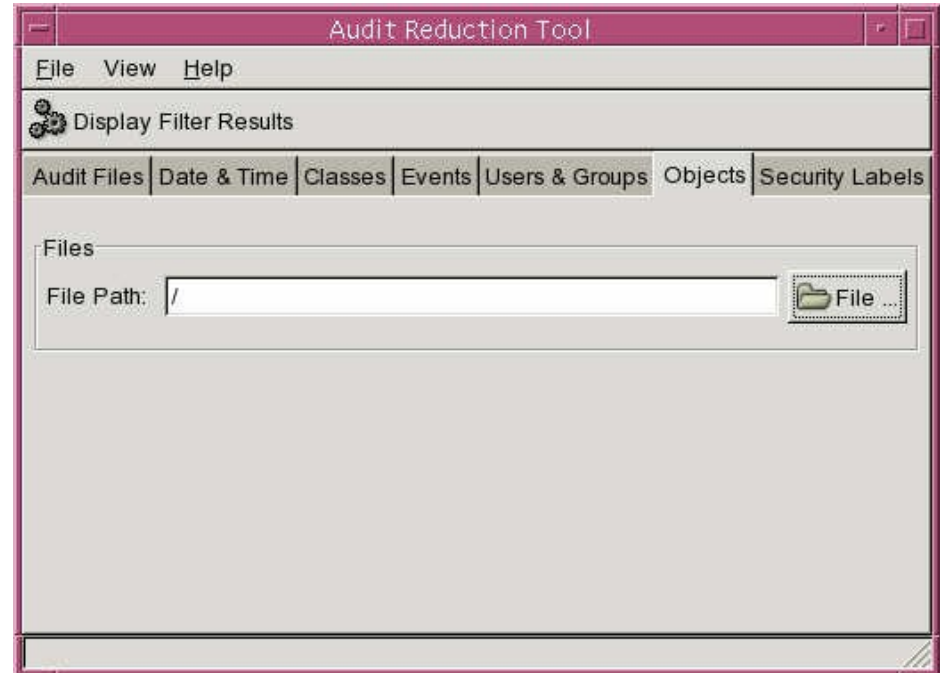


# SecureOffice TWS Administrator TCS System Administration Tools

- Audit Reduction Tool
  - Users & Groups Selection
    - Select Real or Effective Users for review
    - Select Real Group for review

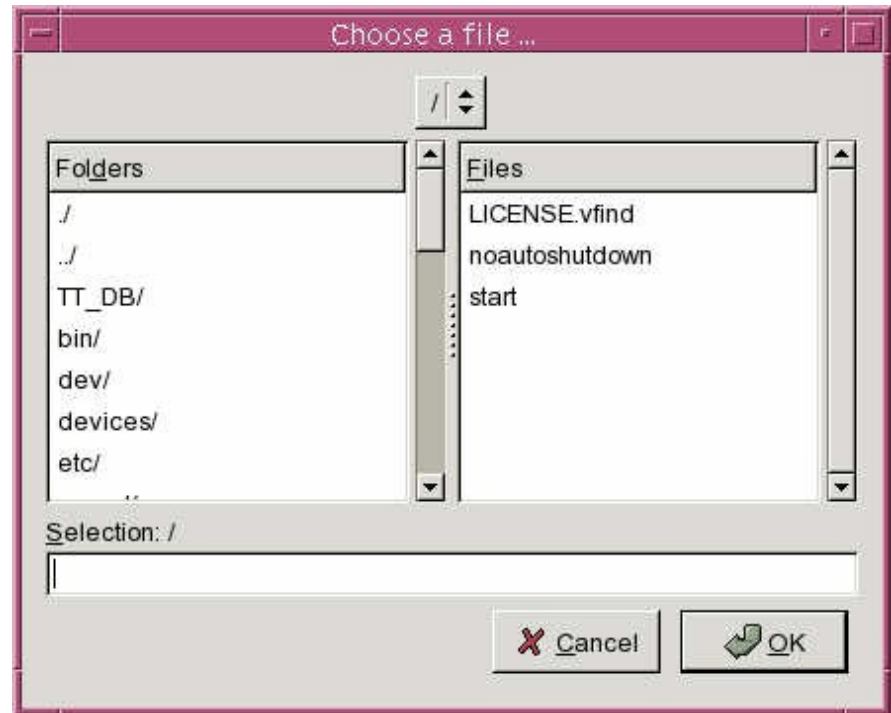


- Audit Reduction Tool
  - Object Selection
    - Select individual file for audit record search



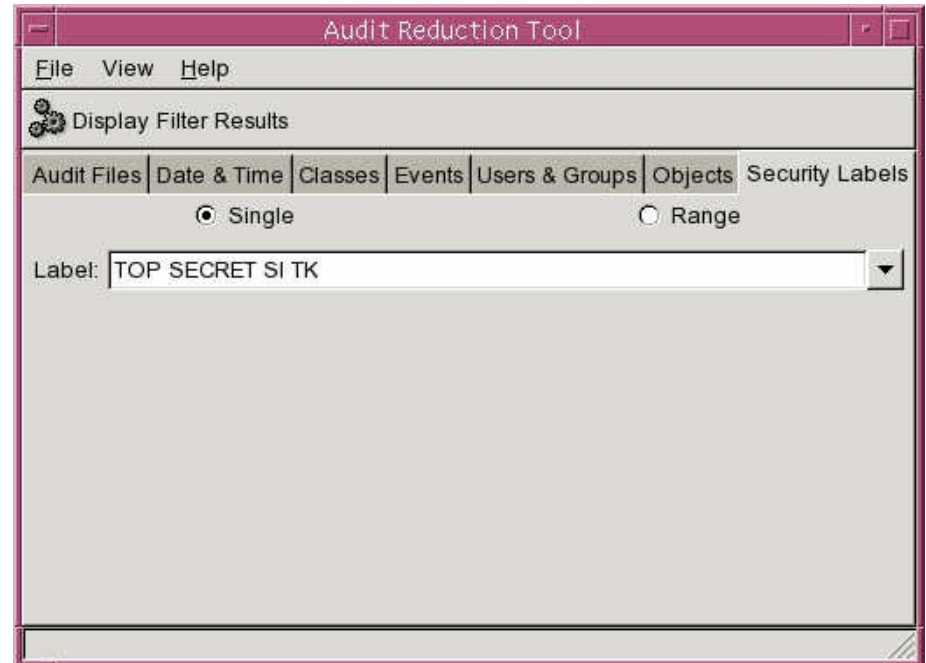
# SecureOffice TWS Administrator TCS System Administration Tools

- Audit Reduction Tool
  - File selection dialog



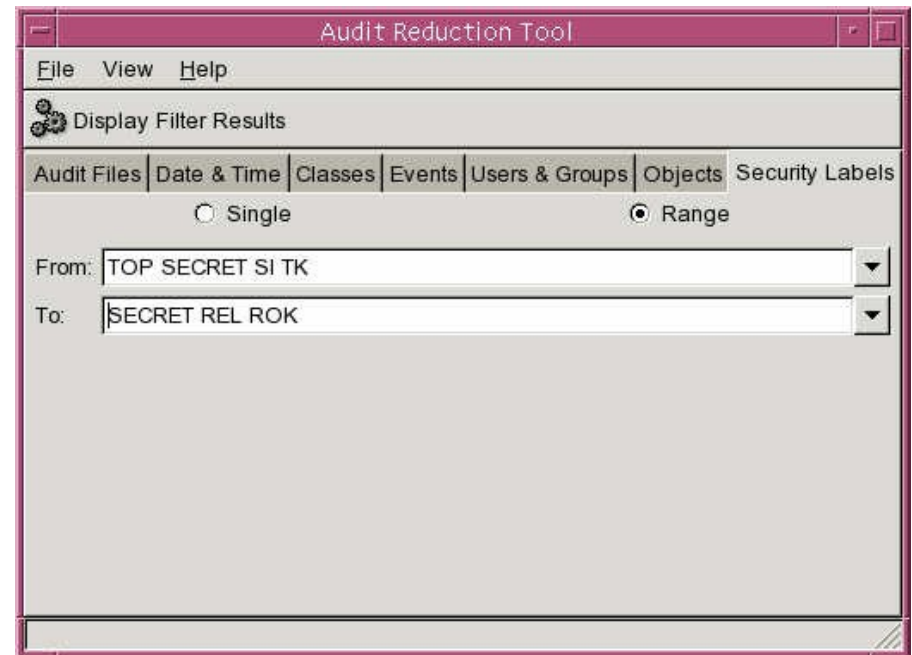
# SecureOffice TWS Administrator TCS System Administration Tools

- Audit Reduction Tool
  - Security Label selection
    - Allows administrator to select a specific SL or range of SL's to review



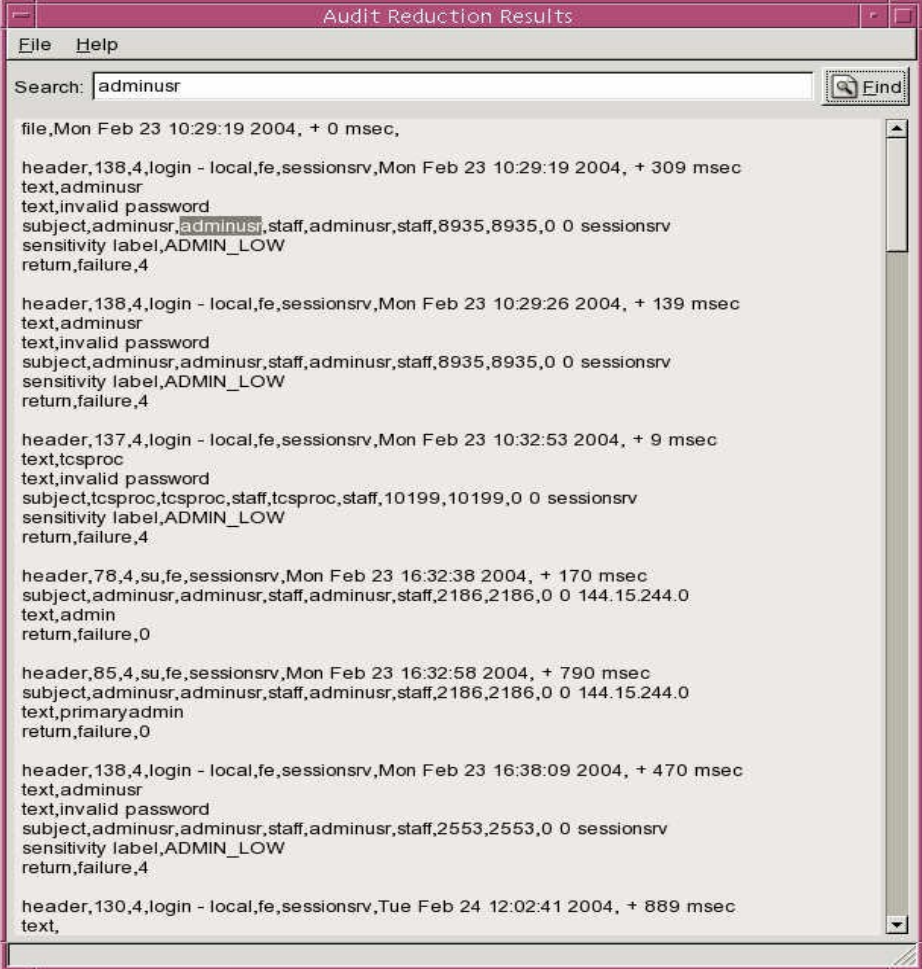
# SecureOffice TWS Administrator TCS System Administration Tools

- Audit Reduction Tool
  - Security Level Selection
    - SL Range selection



# SecureOffice TWS Administrator TCS System Administration Tools

- Audit Reduction Tool
  - Audit record output
  - Human readable format
  - Headers included to increase readability



A screenshot of the 'Audit Reduction Results' window. The window has a menu bar with 'File' and 'Help'. Below the menu bar is a search bar with the text 'adminusr' and a 'Find' button. The main area displays a list of audit records, each starting with a header line indicating the date and time. The records show various events such as login attempts, password validation, and session management. The records are as follows:

```
file,Mon Feb 23 10:29:19 2004, + 0 msec,  
  
header,138,4,login - local,fe,sessionsrv,Mon Feb 23 10:29:19 2004, + 309 msec  
text,adminusr  
text,invalid password  
subject,adminusr,adminusr,staff,adminusr,staff,8935,8935,0 0 sessionsrv  
sensitivity label,ADMIN_LOW  
return,failure,4  
  
header,138,4,login - local,fe,sessionsrv,Mon Feb 23 10:29:26 2004, + 139 msec  
text,adminusr  
text,invalid password  
subject,adminusr,adminusr,staff,adminusr,staff,8935,8935,0 0 sessionsrv  
sensitivity label,ADMIN_LOW  
return,failure,4  
  
header,137,4,login - local,fe,sessionsrv,Mon Feb 23 10:32:53 2004, + 9 msec  
text,tcsproc  
text,invalid password  
subject,tcsproc,tcsproc,staff,tcsproc,staff,10199,10199,0 0 sessionsrv  
sensitivity label,ADMIN_LOW  
return,failure,4  
  
header,78,4,su,fe,sessionsrv,Mon Feb 23 16:32:38 2004, + 170 msec  
subject,adminusr,adminusr,staff,adminusr,staff,2186,2186,0 0 144.15.244.0  
text,admin  
return,failure,0  
  
header,85,4,su,fe,sessionsrv,Mon Feb 23 16:32:58 2004, + 790 msec  
subject,adminusr,adminusr,staff,adminusr,staff,2186,2186,0 0 144.15.244.0  
text,primaryadmin  
return,failure,0  
  
header,138,4,login - local,fe,sessionsrv,Mon Feb 23 16:38:09 2004, + 470 msec  
text,adminusr  
text,invalid password  
subject,adminusr,adminusr,staff,adminusr,staff,2553,2553,0 0 sessionsrv  
sensitivity label,ADMIN_LOW  
return,failure,4  
  
header,130,4,login - local,fe,sessionsrv,Tue Feb 24 12:02:41 2004, + 889 msec  
text,
```

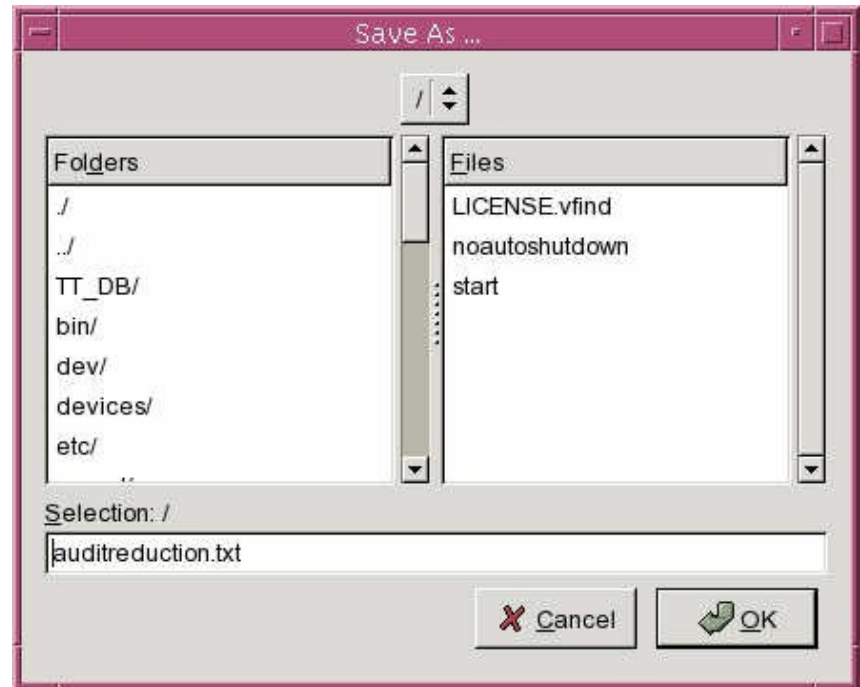


# SecureOffice TWS

## Administrator

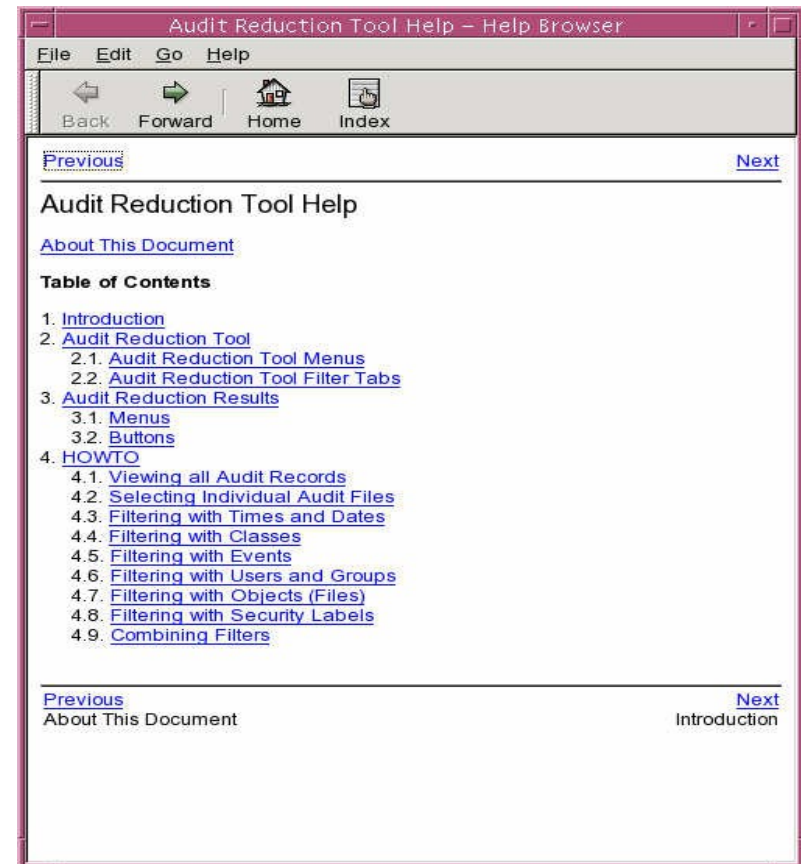
### TCS System Administration Tools

- Audit Reduction Tool
  - Export to File
  - 'Save As' dialog
  - Records are saved at ADMIN\_HIGH security level



# SecureOffice TWS Administrator TCS System Administration Tools

- Audit Reduction Tool
  - Interactive Help Menu

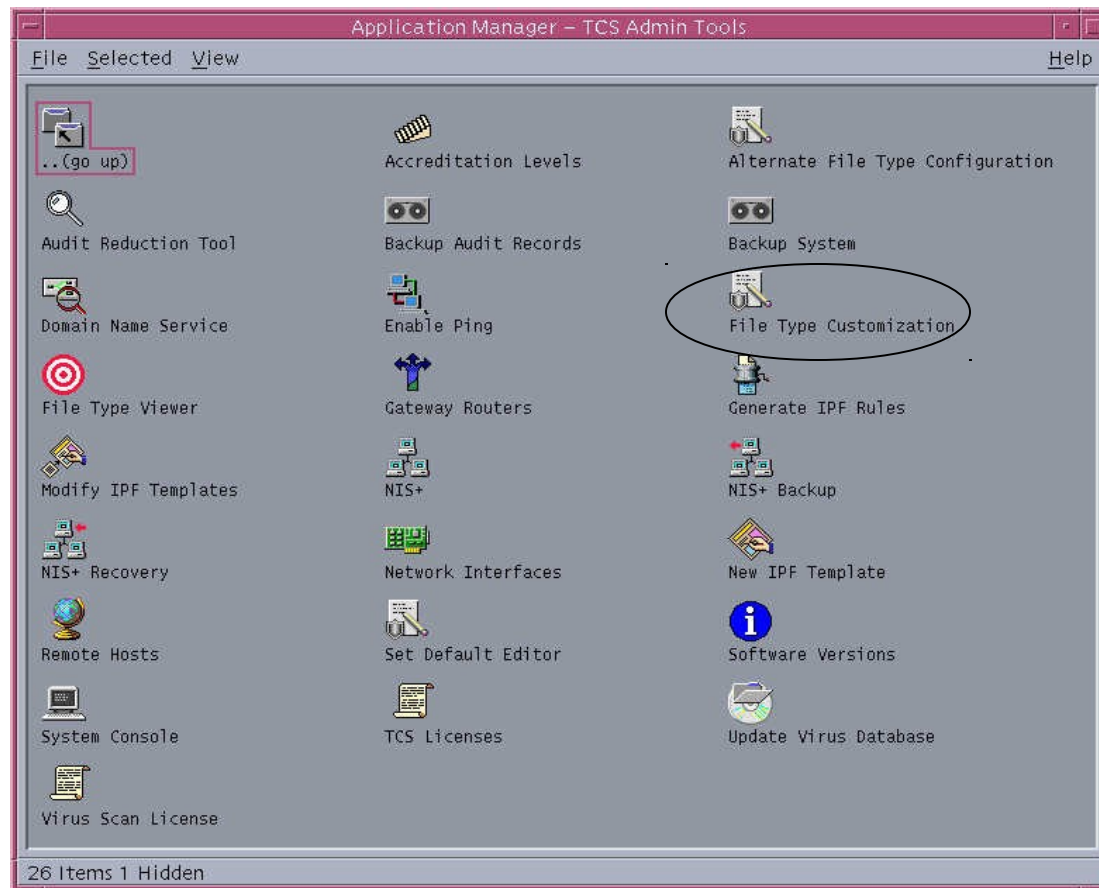


- Audit Reduction Tool
  - Version



# SecureOffice TWS Administrator TCS System Administration Tools

## File Type Customization Tool

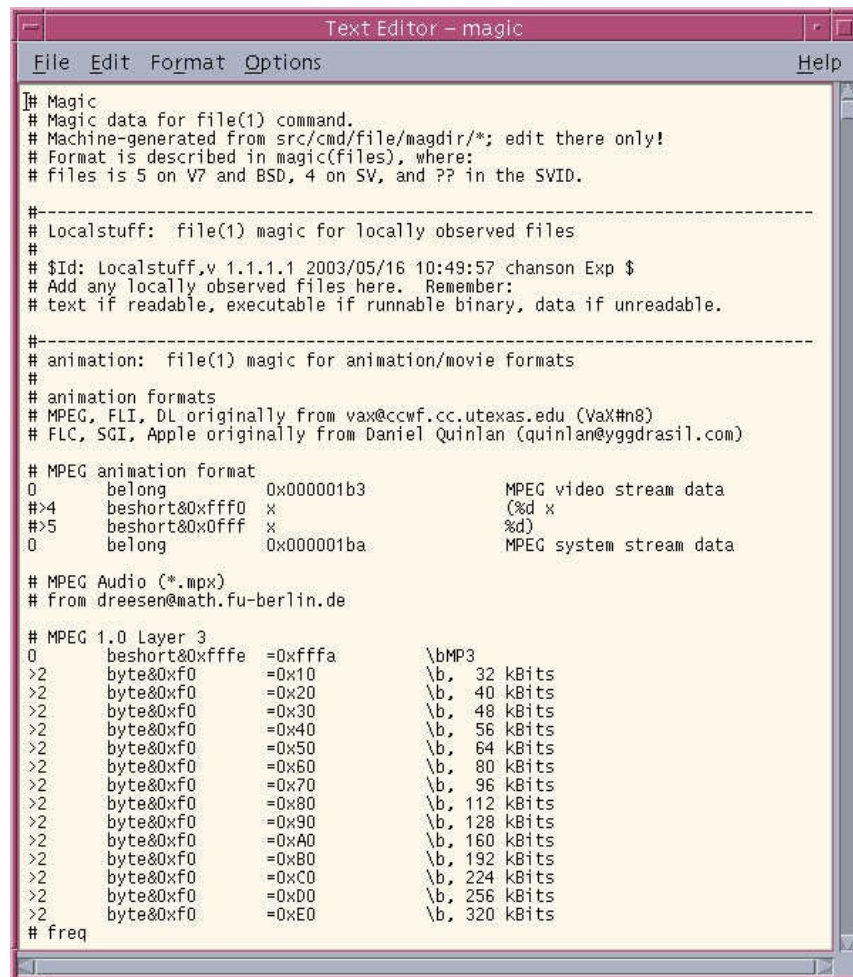


# SecureOffice TWS

## Administrator

### TCS System Administration Tools

- File Type Customization Tool
  - Allows administrator to define the MIME Magic file for the Trusted File Relabeler file typing function



```
Text Editor - magic
File Edit Format Options Help

[]# Magic
[]# Magic data for file(1) command.
[]# Machine-generated from src/cmd/file/magdir/*; edit there only!
[]# Format is described in magic(files), where:
[]# files is 5 on V7 and BSD, 4 on SV, and ?? in the SVId.

[]#-----
[]# Localstuff: file(1) magic for locally observed files
[]#
[]# $Id: Localstuff.v 1.1.1.1 2003/05/16 10:49:57 chanson Exp $
[]# Add any locally observed files here. Remember:
[]# text if readable, executable if runnable binary, data if unreadable.
[]#-----
[]# animation: file(1) magic for animation/movie formats
[]#
[]# animation formats
[]# MPEG, FLI, DL originally from vax@ccwf.cc.utexas.edu (VaX#n8)
[]# FLC, SGI, Apple originally from Daniel Quinlan (quinlan@yggdrasil.com)

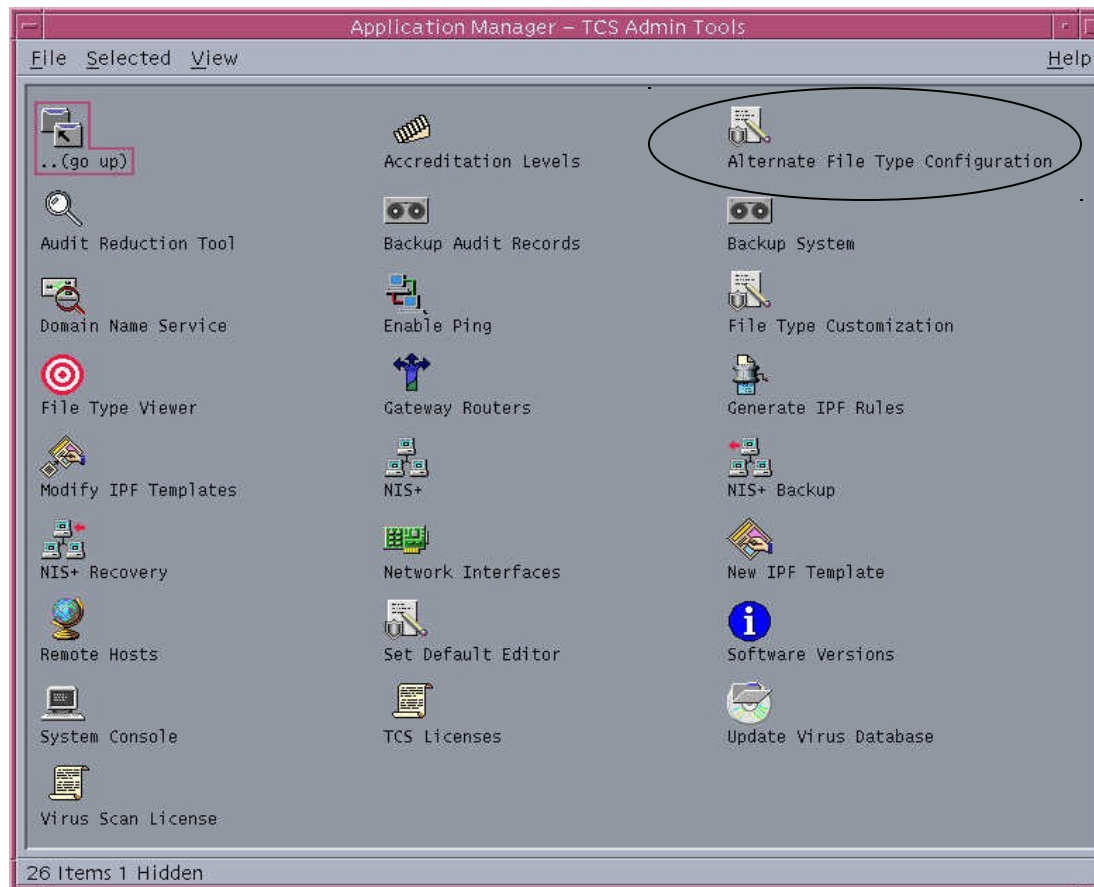
[]# MPEG animation format
0      belong      0x000001b3      MPEG video stream data
#>4    beshort&0xffff x          (%d x
#>5    beshort&0xffff x          (%d)
0      belong      0x000001ba      MPEG system stream data

[]# MPEG Audio (*.mpx)
[]# from dreessen@math.fu-berlin.de

[]# MPEG 1.0 Layer 3
0      beshort&0xfffe =0xffffa    \bMP3
>2     byte&0xf0      =0x10      \b, 32 kBits
>2     byte&0xf0      =0x20      \b, 40 kBits
>2     byte&0xf0      =0x30      \b, 48 kBits
>2     byte&0xf0      =0x40      \b, 56 kBits
>2     byte&0xf0      =0x50      \b, 64 kBits
>2     byte&0xf0      =0x60      \b, 80 kBits
>2     byte&0xf0      =0x70      \b, 96 kBits
>2     byte&0xf0      =0x80      \b, 112 kBits
>2     byte&0xf0      =0x90      \b, 128 kBits
>2     byte&0xf0      =0xA0      \b, 160 kBits
>2     byte&0xf0      =0xB0      \b, 192 kBits
>2     byte&0xf0      =0xC0      \b, 224 kBits
>2     byte&0xf0      =0xD0      \b, 256 kBits
>2     byte&0xf0      =0xE0      \b, 320 kBits
[]# freq
```

# SecureOffice TWS Administrator TCS System Administration Tools

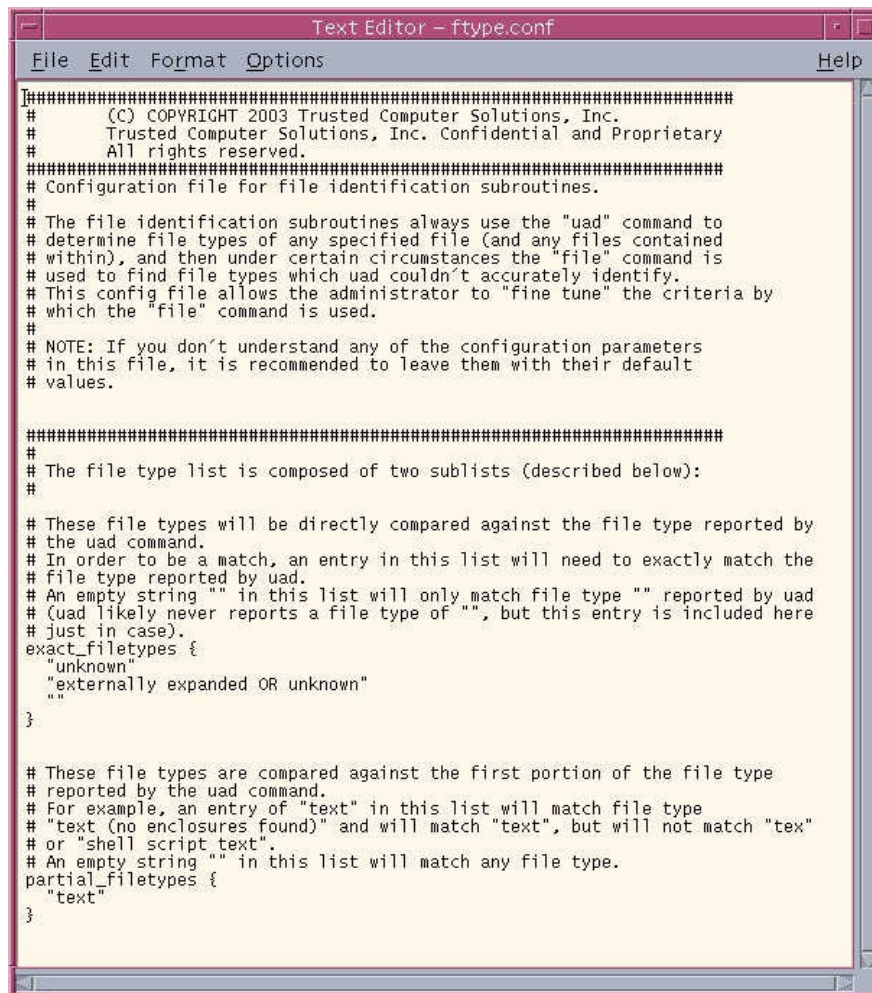
## Alternate File Type Customization Tool





# SecureOffice TWS Administrator TCS System Administration Tools

- Alternate File Type Configuration Tool
  - Additional customization for MIME Magic files



```
Text Editor - ftype.conf
File Edit Format Options Help

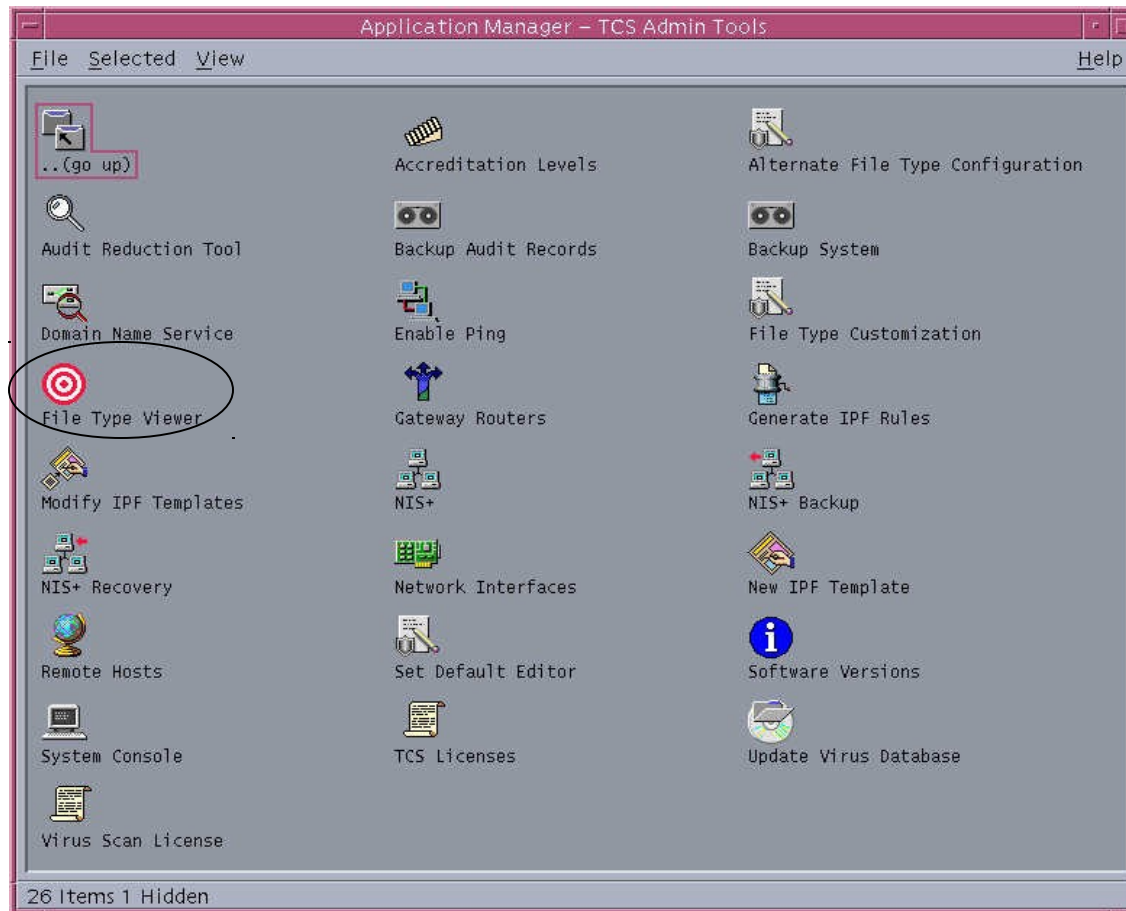
#####
# (C) COPYRIGHT 2003 Trusted Computer Solutions, Inc.
# Trusted Computer Solutions, Inc. Confidential and Proprietary
# All rights reserved.
#####
# Configuration file for file identification subroutines.
#
# The file identification subroutines always use the "uad" command to
# determine file types of any specified file (and any files contained
# within), and then under certain circumstances the "file" command is
# used to find file types which uad couldn't accurately identify.
# This config file allows the administrator to "fine tune" the criteria by
# which the "file" command is used.
#
# NOTE: If you don't understand any of the configuration parameters
# in this file, it is recommended to leave them with their default
# values.

#####
#
# The file type list is composed of two sublists (described below):
#
# These file types will be directly compared against the file type reported by
# the uad command.
# In order to be a match, an entry in this list will need to exactly match the
# file type reported by uad.
# An empty string "" in this list will only match file type "" reported by uad
# (uad likely never reports a file type of "", but this entry is included here
# just in case).
exact_filetypes {
    "unknown"
    "externally expanded OR unknown"
    ""
}

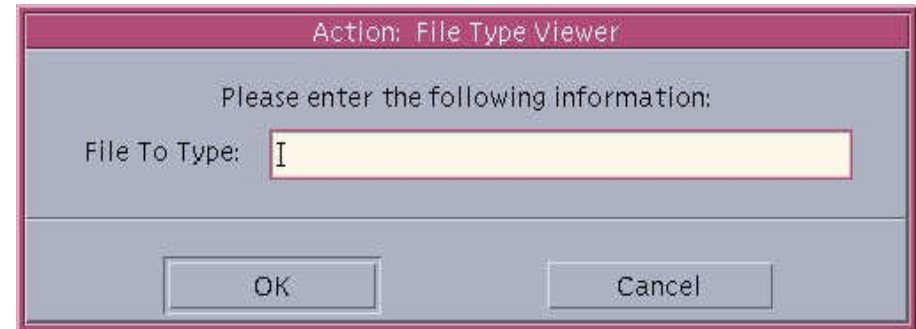
# These file types are compared against the first portion of the file type
# reported by the uad command.
# For example, an entry of "text" in this list will match file type
# "text (no enclosures found)" and will match "text", but will not match "tex"
# or "shell script text".
# An empty string "" in this list will match any file type.
partial_filetypes {
    "text"
}
```

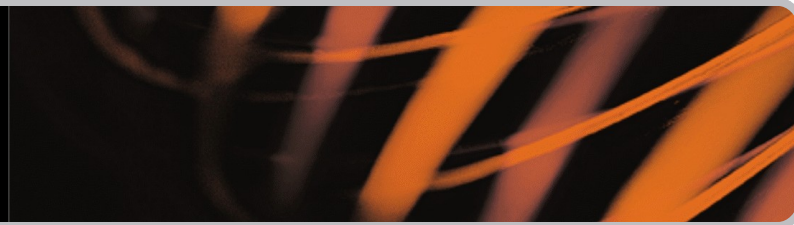
# SecureOffice TWS Administrator TCS System Administration Tools

## File Type Viewer



- File Type Viewer Tool
  - Allows the administrator to determine the file type of any file on the system
  - Files must be stored in a Single Level Directory to be typed





- TCS Administration Tools Review
  - Questions?
- Module Three : SecureOffice Trusted Workstation Administration Tools